华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：*关联证书*后，请提交您的“华为账号”和注册账号的“email”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见*LVC排期*
- **4、学习工具 eNSP**
  - eNSP (Enterprise Network Simulation Platform), 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）



HC120320001
终端安全概述

www.huawei.com

HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解终端安全当前的主要现状；
  - 了解终端安全的产生背景；
  - 了解终端安全解决思路-立体防御体系。

本章是终端安全概述，核心知识点：终端安全解决思路-立体防御体系



目录



终端安全现状

安全威胁出现频度对比，2007 年

来源：IDC, 2007

安全威胁	(%)
病毒、特洛伊木马及恶意代码	96.1
垃圾邮件	55.9
间谍软件	33.3
应用程序的漏洞	31.6
黑客入侵	22.1
内部员工破坏IT系统	8.1
无线网络带来的安全问题	8.1
内部雇员或者合作伙伴偷窃数据	7.8

IDC统计报告

形同虚设?

Enterprise

文件服务器

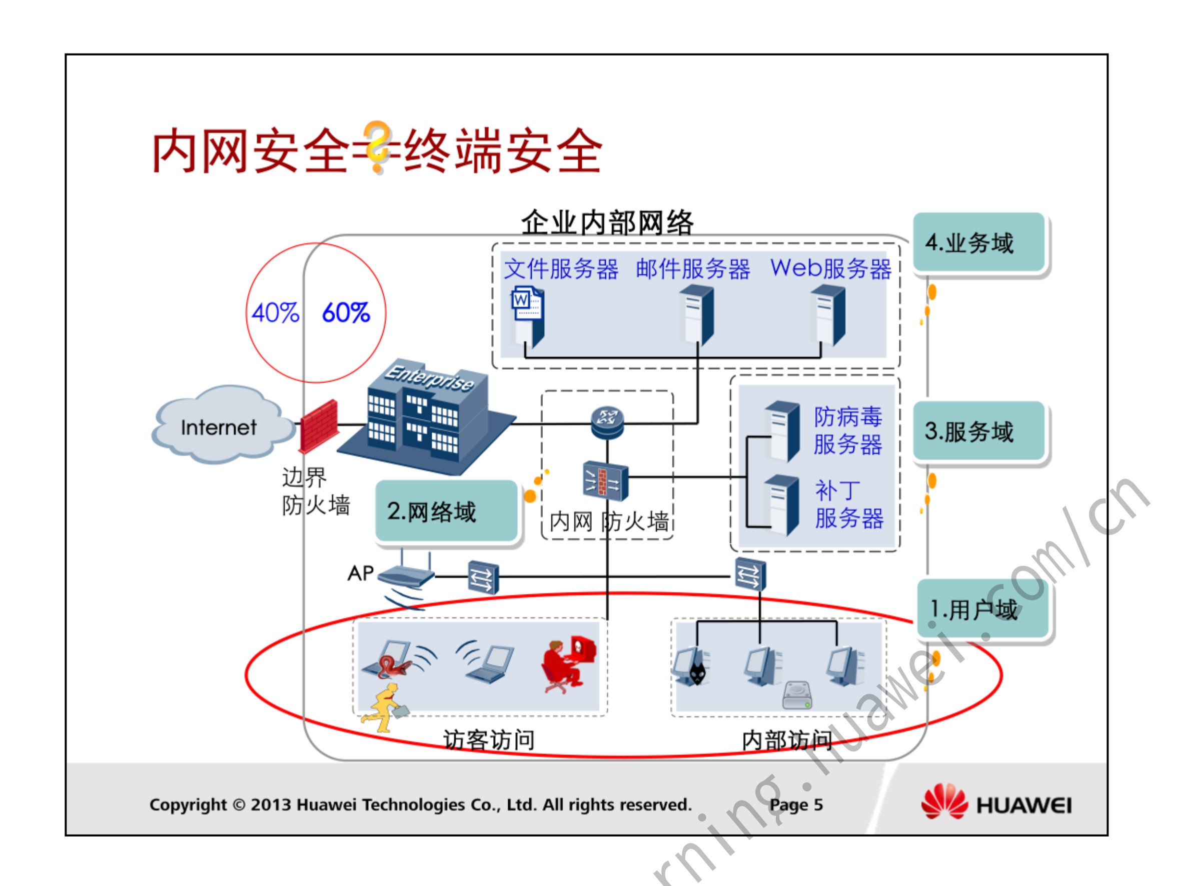
邮件服务器

WEB服务器

- **内网安全主要威胁**
  - 存储介质滥用与失窃
  - 未授权访问
  - 重要信息资产泄密
  - 病毒及恶意代码

据IDC统计报告计算机犯罪与安全调查显示，存储介质滥用与失窃、未授权访问、重要信息资产泄密、IT系统漏洞、病毒及恶意代码、 IM即时通讯软件和非工作时间的Web访问已经成为企业面临的最严重的安全威胁之一。而目前企业信息安全建设现状是，企业在严防死守外部黑客和病毒攻击的同时，却忽略了内部威胁。从2大组织显示的报告得知，有大量的企业内部安全威胁正在对企业重要的信息资产造成严重的影响。

因此，传统的边界防护措施在越来越多的内网安全风险面前，呈现出“形同虚设”态势。所以，企业IT管理人员需要逐步将工作中心向内网安全防护转移。

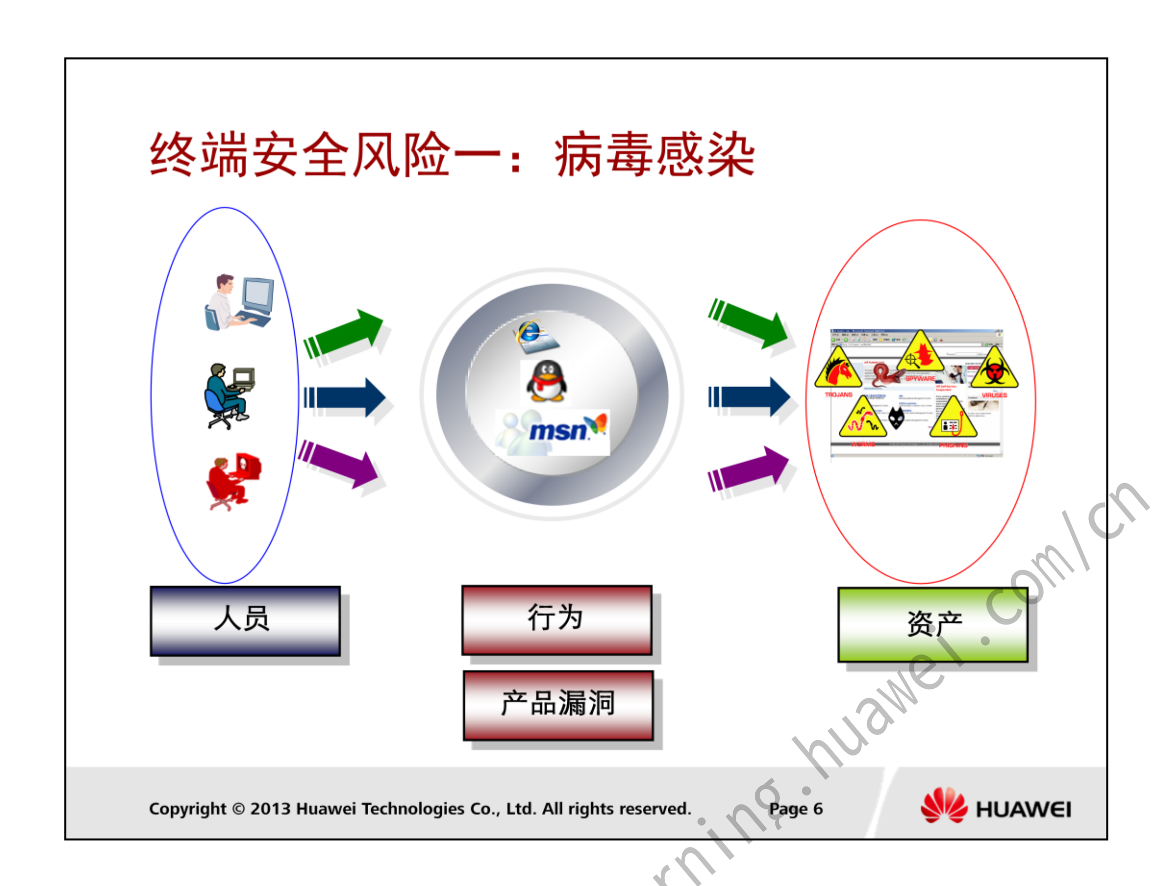


据IDC统计报告和CSI/FBI 计算机犯罪与安全调查显示，60%以上安全事件来自于内网。那么我们首先要澄清“什么是安全域划分及边界整合”、“什么是内网安全”、“什么是终端安全”、“内网安全是否等同于终端安全”等概念。

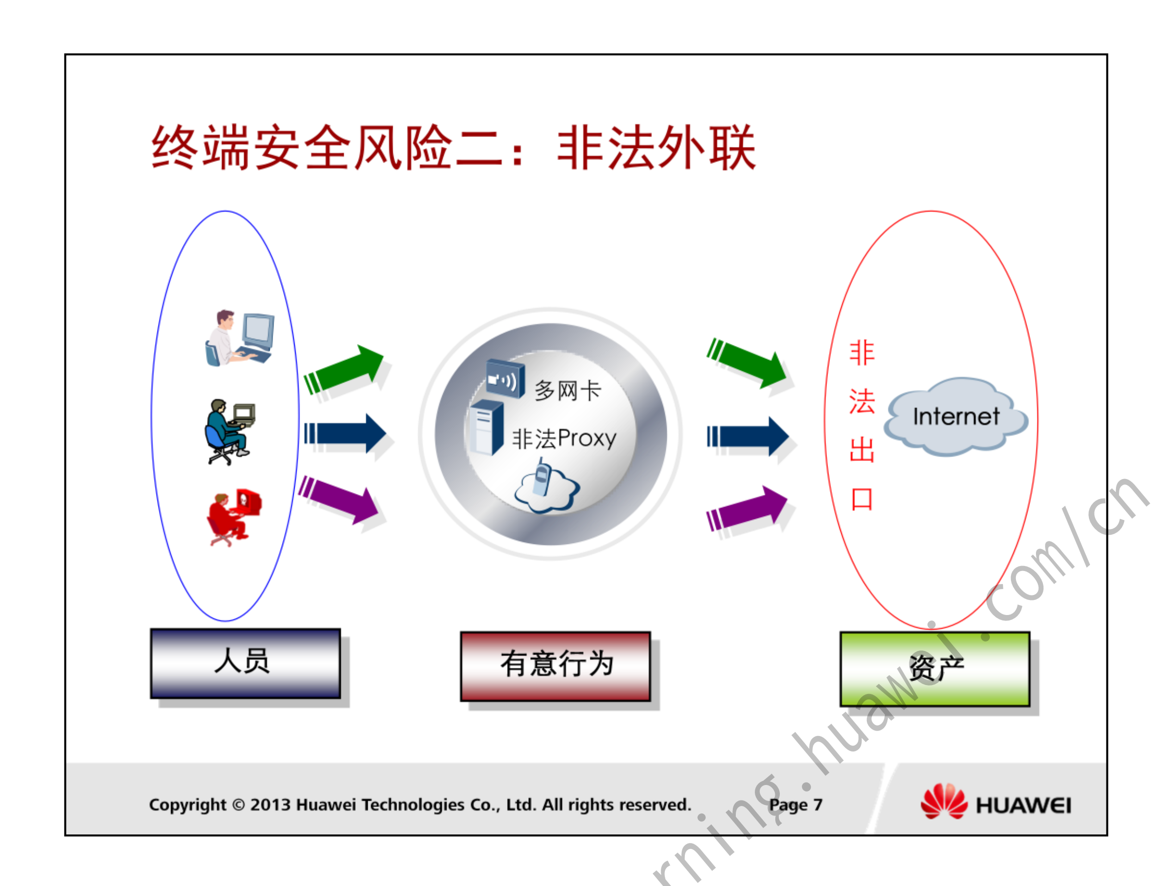
所谓安全域划分及边界整合涉及两方面，即安全域划分和边界整合，其中安全域划分是指为了更好保障内网安全，基于内网业务类型和安全需求，把内网划分成若干个颗粒度合适的逻辑区域。而边界整合是指为了降低企业内网与外部网络或Internet互联可能带来的安全风险，对企业内网所有的互联接口进行整合，实现统一防护、统一监控的目的。安全域主要由用户域、网络域、服务域、业务域等4大安全区域组成。其中用户域安全一般由各类终端用户组成，由于终端所具有的数量大、分布广、流动强等特点，导致其是4大安全区域中最重要控制的区域，也是本教材讲解的重要，即终端安全。网络域安全，是业务流量承载的平台，一般情况下通过采用MPLS VPN技术把业务根据企业的要求进行逻辑划分，以实现网络承载的安全。服务域安全，是为企业内网提供安全服务的区域，此区域一般由防病毒服务器、补丁管理服务器、终端安全服务器等提供安全服务的系统组成。业务域安全，即企业业务服务器的安全，是各类企业最关注的安全防护区域，其承载着企业重要的、核心的信息资产。

通过对“安全域划分及边界整合”概念的澄清，我们就好地对内网安全进行定义。内网安全，是指通过综合的安全解决方案，保障用户域、网络域、服务域和业务域等4大区域的安全，终端安全，是采用立体防御理念形成体系化的产品、解决方案和服务。

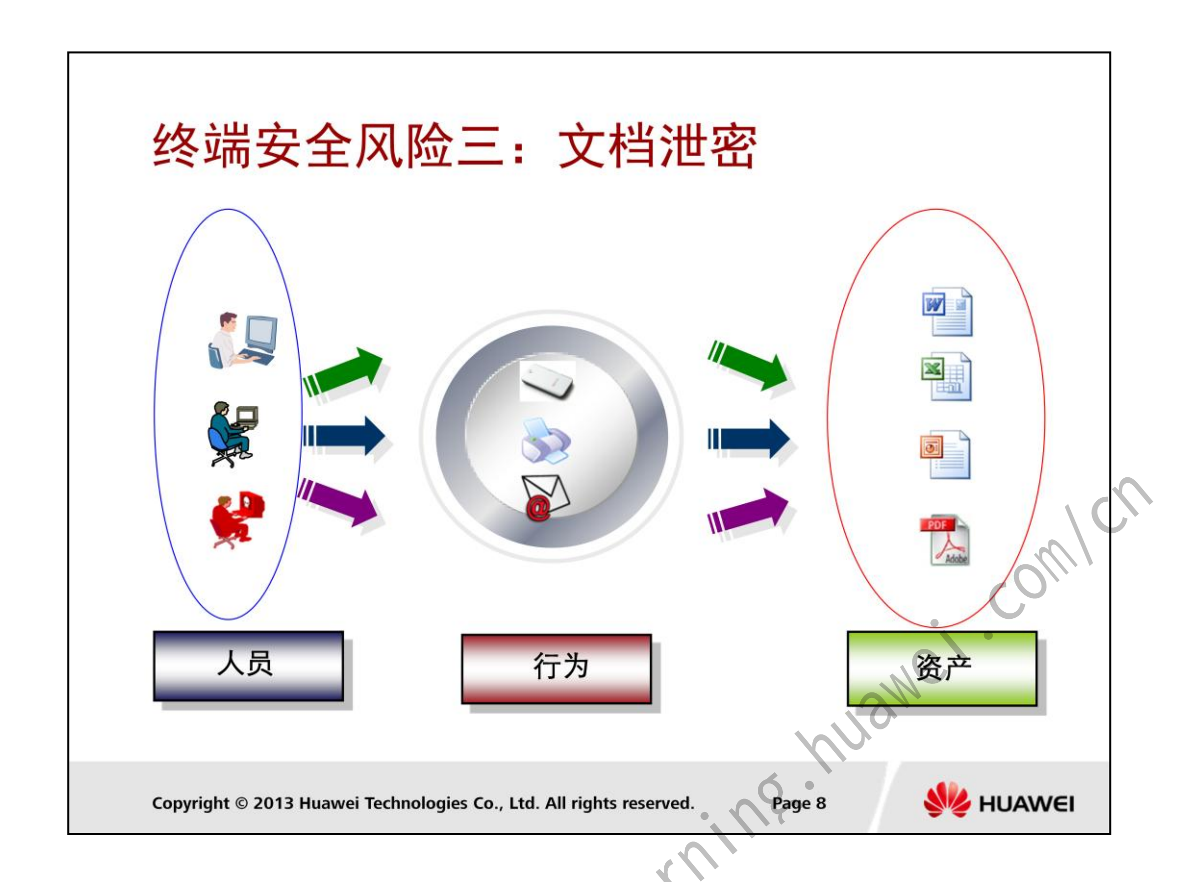
通过对“内网安全”和“终端安全”的定义，我们知道终端安全是内网安全的一部分，且因终端所具有的特点，致使其为内网最难以防护的安全区域和安全隐患的源头。



终端安全风险一，因终端自身存在的系统缺陷再加上终端的操作行为，可能会不知不觉感染上病毒。比如通过IE浏览器访问网站，因IE可能存在漏洞，当目标网站挂着病毒时，可能病毒就通过IE漏洞对所在终端进行感染，进而扩散传播。当然还有其它IM工具软件、外设介质均可能充当传播病毒的载体。

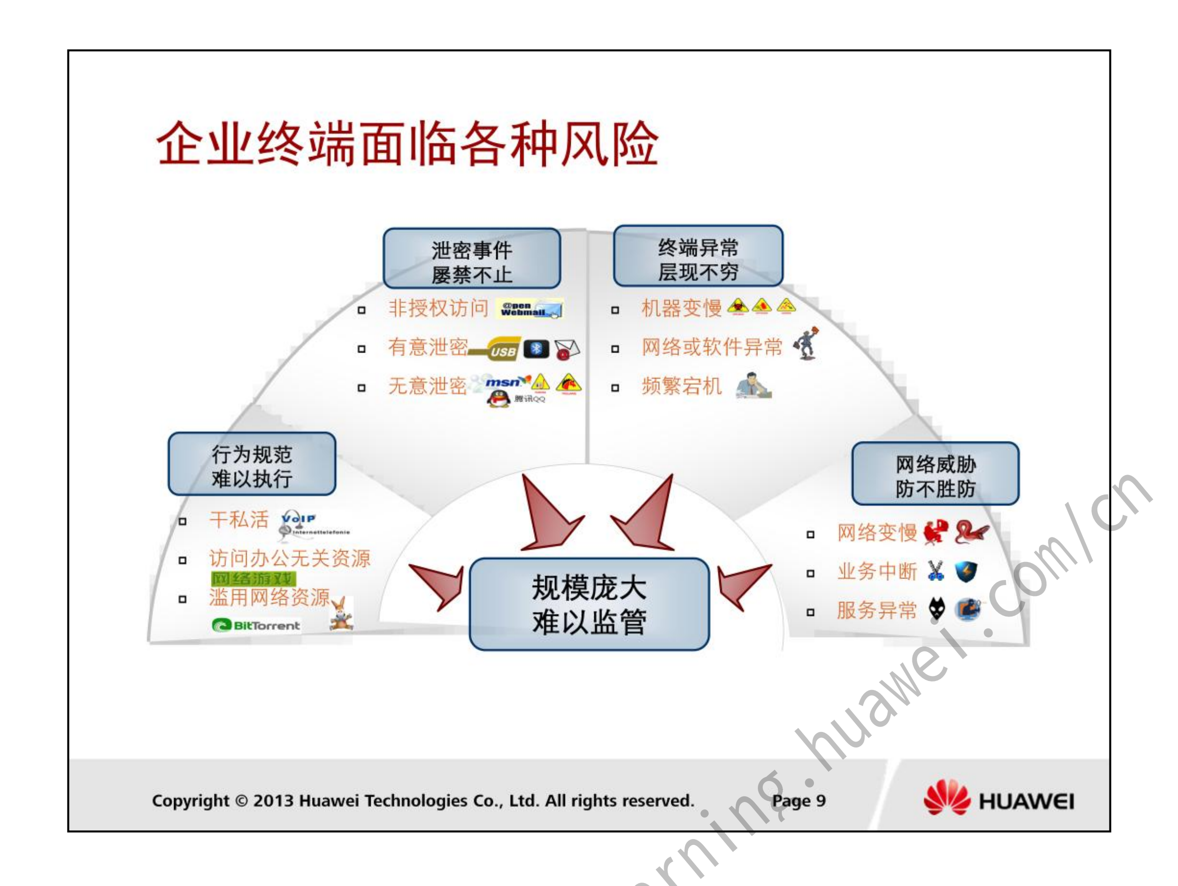


终端安全风险二，此类终端行为一般可归类为有意行为，由于企业信息安全管理和信息安全技术限制，部分终端因无法获取Internet访问资源需求，可能将通过私设访问通道来逃避正常的安全检查。这样除了严重违反企业信息安全管理制度外，还将带来巨大的安全风险。由于通过私设访问通道，一般缺少必要的安全策略机制，往往容易给外部不法分子创造入侵企业内部网络的后门。



终端安全风险三，文档类的信息资产一般是企业重要资产之一，它的泄密将对企业日常运营产生重大影响。而传统控制方式一般不做控制或通过封堵存储介质或外设接口来解决，这除了可能影响终端日常工作效率外，最主要是不能从根本上堵截文档的外泄。比如通过E-mail等方式把文档外发。

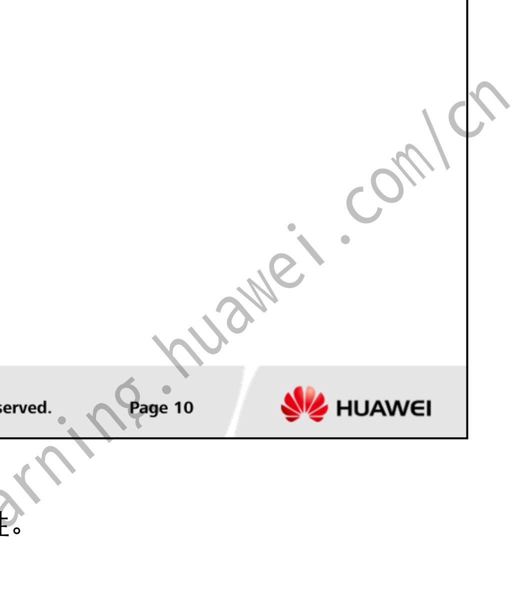
自从Internet快速发展的近十年，内部网络发现的安全事件或案例不仅仅以上列出的三个场景，以上场景只是抛砖引玉来说明一个观点，终端的安全风险已越来越多样化，只有提供整体的解决方案体系平台才是根本。



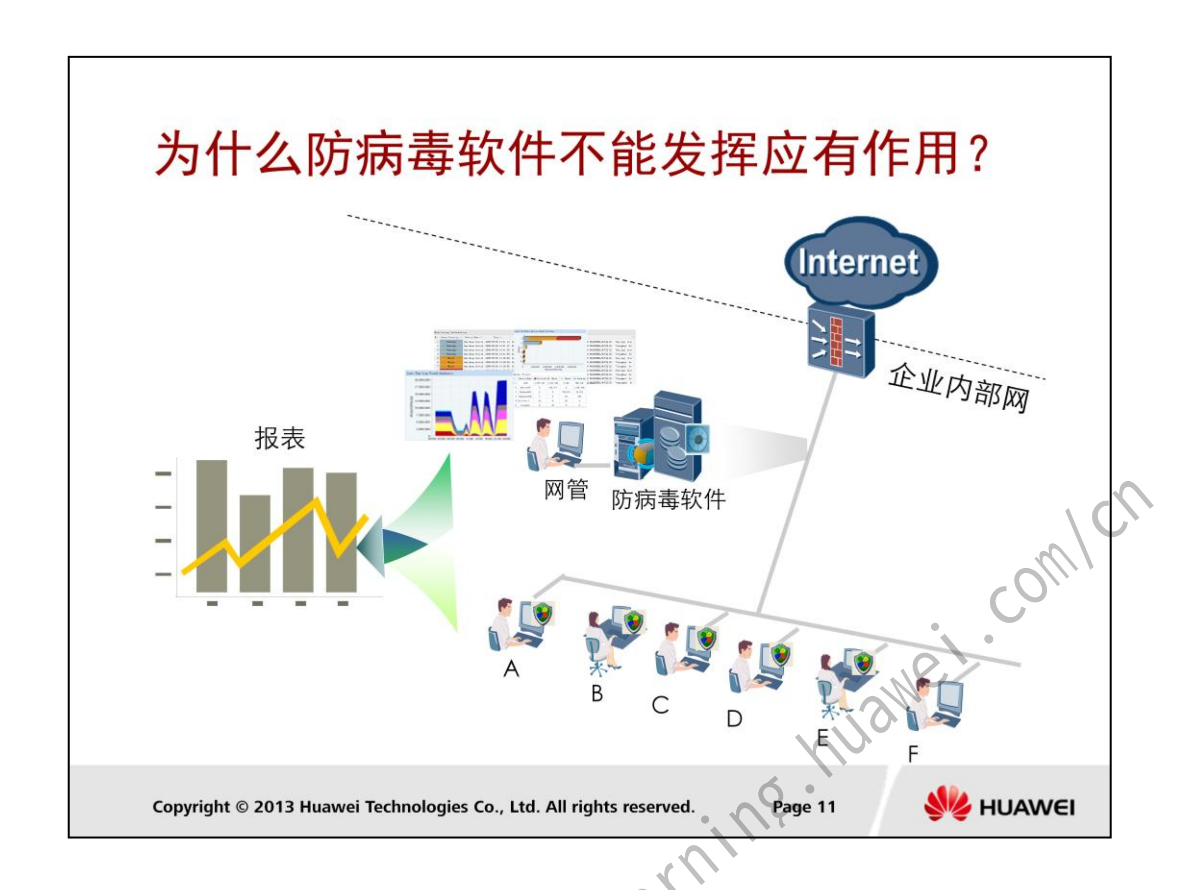
- 企业虽然部署了杀毒软件和安全设备，但是依然存在如下问题。
  - 泄密事件屡禁不止：
  - 非授权访问：外来电脑、跨部门接入电脑、跨权限访问
  - 有意泄密：外设拷贝、聊天、文件传输、资产外出
  - 无意泄密：病毒木马蠕虫、恶意网站、资产丢失
  - 终端异常层现不穷：
  - 病毒、蠕虫、木马、流氓软件导致机器过慢；
  - 恶意代码或入侵事件导致网络或软件异常，使得IT人员沦为疲于奔命的“救火队员
  - 系统破坏、软件冲突导致频繁宕机，使得IT部门形象受损
  - 网络威胁防不胜防：
  - 病毒、蠕虫、源自终端的恶意攻击（入网络剪刀手、网络执法官等、ARP攻击）、网络资源滥用导致网络变慢甚至业务终端或应用系统异常



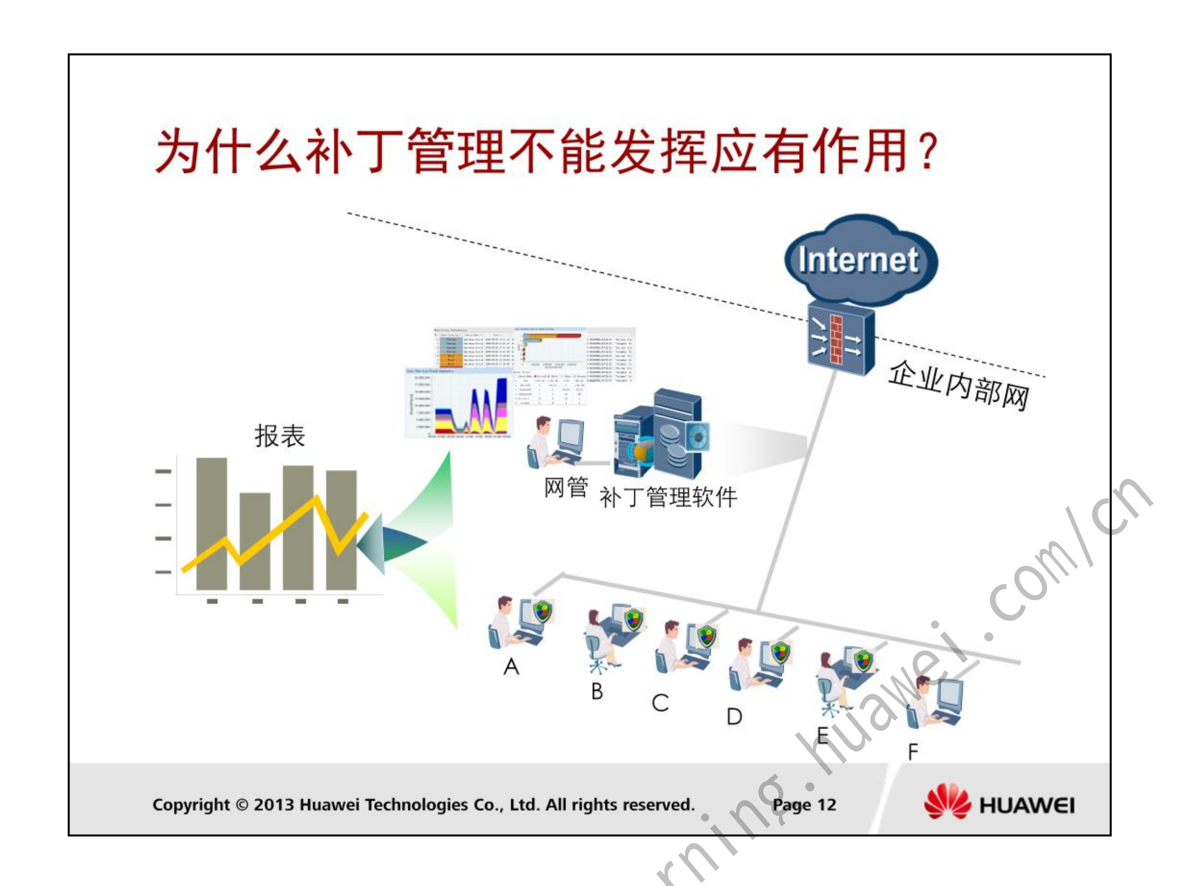
目录



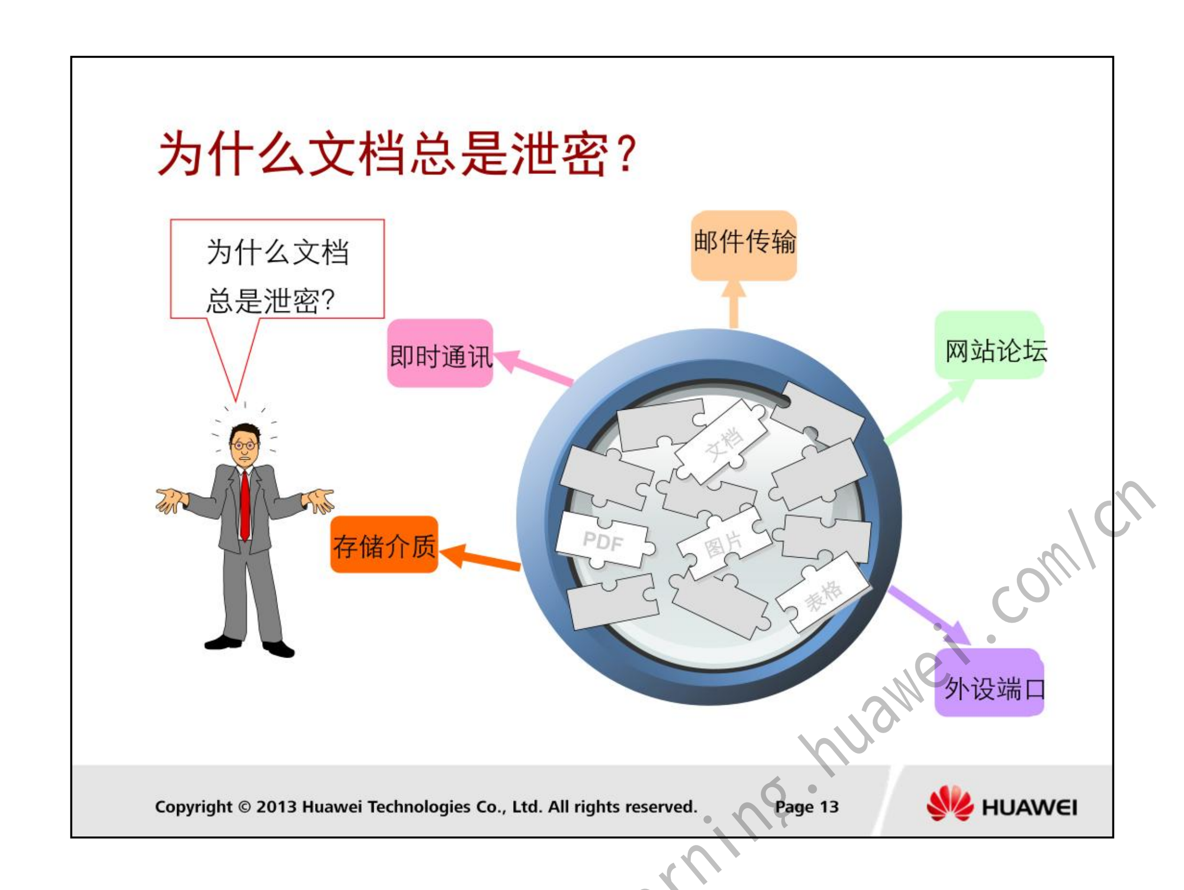
本节主要介绍传统终端安全解决方案的局限性。



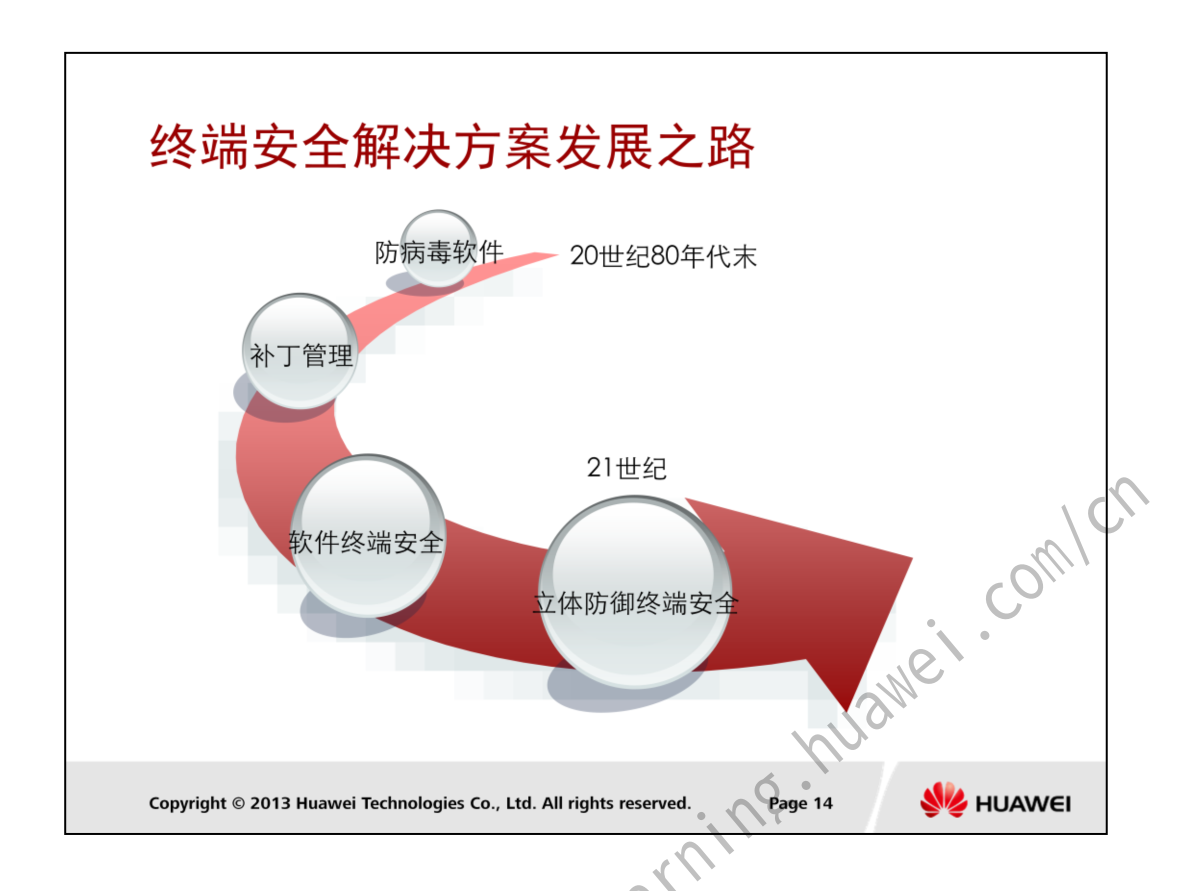
防病毒软件发挥应有作用的前提，各终端除了需保持软件运行外，防病毒软件版本、引擎及病毒库均需保持最新。但由于单一的防病毒软件的局限性，使其很难保证网内所有终端防病毒软件信息的统一。比如防病毒软件随意卸载、安装非企业统一品牌防病毒软件、病毒库未及时更新升级等等，这些现象在当前的企业内部网络特别普遍，致使传统的防病毒软件不能发挥应有的作用。以下章节，将阐述如何把立体防御终端安全解决方案与防病毒软件进行整合，以还原防病毒软件应有的本色。



相对于防病毒软件，补丁管理实现机制比较简单。一般情况下，补丁管理代理端软件都是嵌入终端系统内，只需保证补丁的及时下发、安装就行。但由于补丁实现机制原因，都会有部分重要补丁因各种原因而未能及时下发，从而引起终端弱点的产生。这些现象与防病毒软件一样，都使补丁管理不能发挥应有的作用。以下章节，将阐述如何把立体防御终端安全解决方案与补丁管理进行整合，以还原补丁管理应有的本色。



传统解决文档泄密技术往往考虑如何阻止文档向外传输接口，但由于接口类型与数量多，且承载在IP协议之上的传输协议技术不好控制，致使此类解决方案均存在这样那样缺陷，最终导致文档频繁泄密，而且针对文档的合法用户如何有效地进行权限控制及访问，此类措施均存在这样那样的问题。因此从源头解决文档的安全、合法、合理使用是当前解决方案的首推之选。以下章节，将阐述如何对文档进行多层次防护和源头防护，来解决文档所存在的泄密问题。



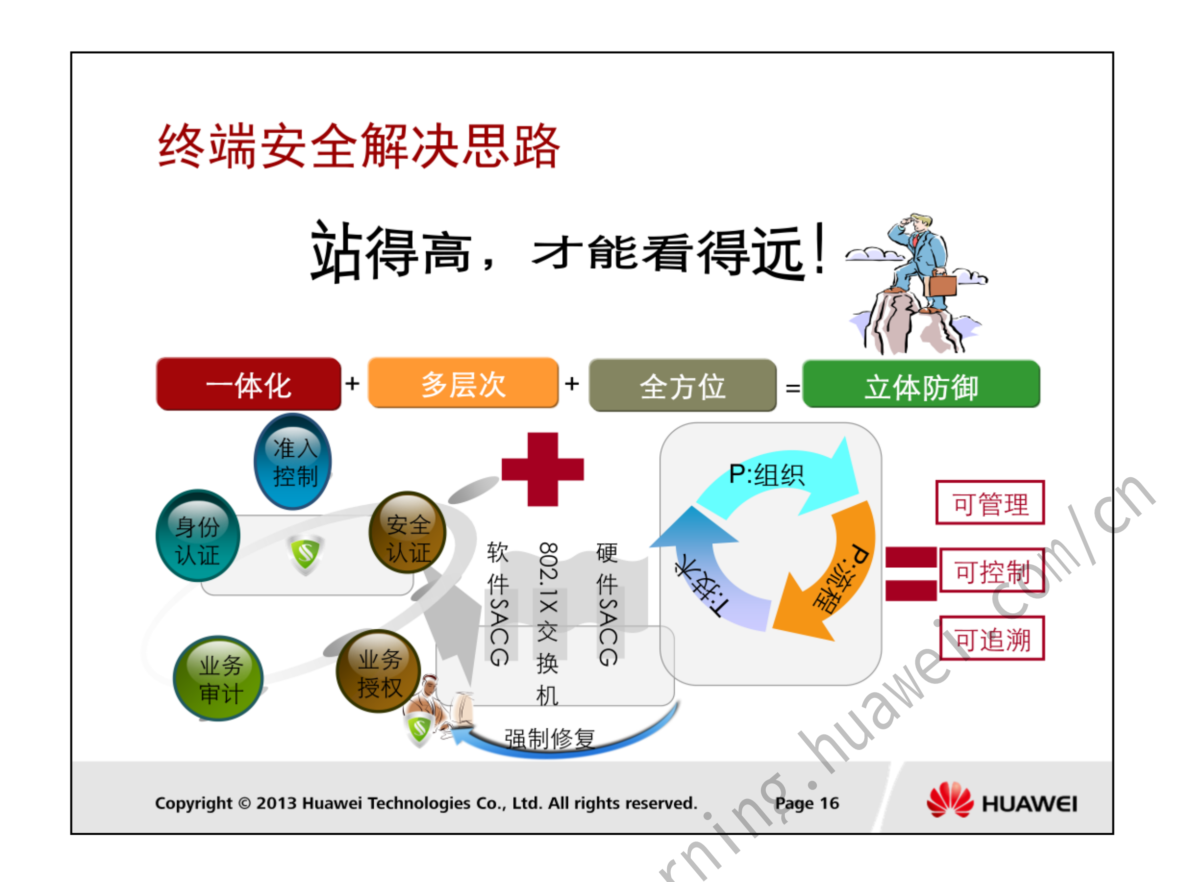
以下我们来简要阐述一下，终端安全解决方案发展之路。终端安全解决方案诞生最早可追溯至20世纪80年代真正意义的病毒产生，当时IT界联网还未形成，基本上处于孤岛阶段。风险来源主要还是病毒，且承载介质也是以外设为主，所以当时解决方案主要还是以单一的防病毒软件。伴随着互联网的产生，越来越多的终端通过Internet联接在一起，这样在带来方便性的同时，许多安全威胁也跟随而来。这时终端用户除了安装防病毒软件，还不定期地对终端系统进行补丁修复。进入了21世纪，企业信息化对企业的经营越来越重要，随后各类企业逐步建立了各自的企业内网，但安全问题却越来越多，如何解决这些终端问题是各企业IT经理人所关心的难题，这时有部分软件厂商或防病毒厂商介入终端安全领域，经过近十年的发展，大家感觉单纯的软件终端安全解决方案难以从根本上解决企业所面临的终端安全问题，急需提供一套主动的、动态的、纵深的解决方案才是解决之道。

立体防御终端安全解决方案就浮出历史舞台，它整合了原有的系统层面终端安全技术，又延伸新的网络层面技术，从而全面地解决终端所面临的各类安全问题。

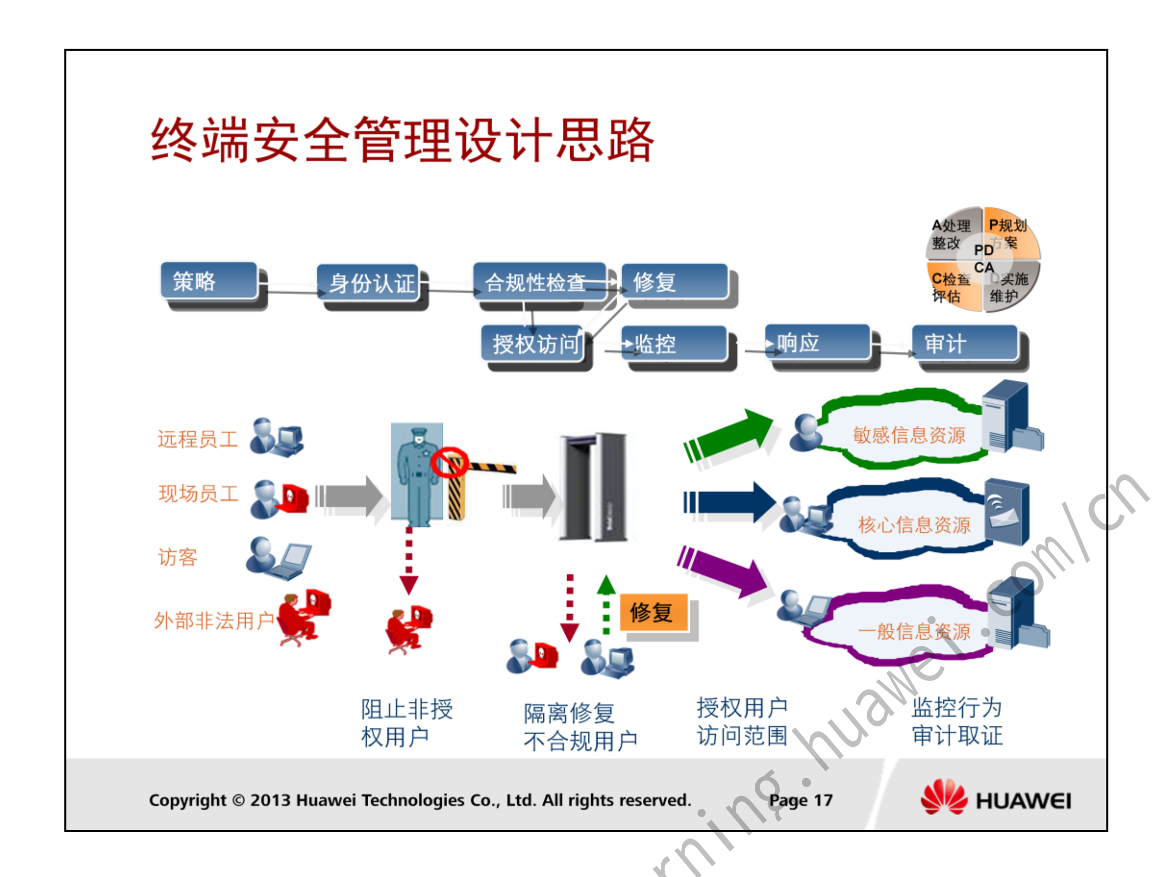


目录

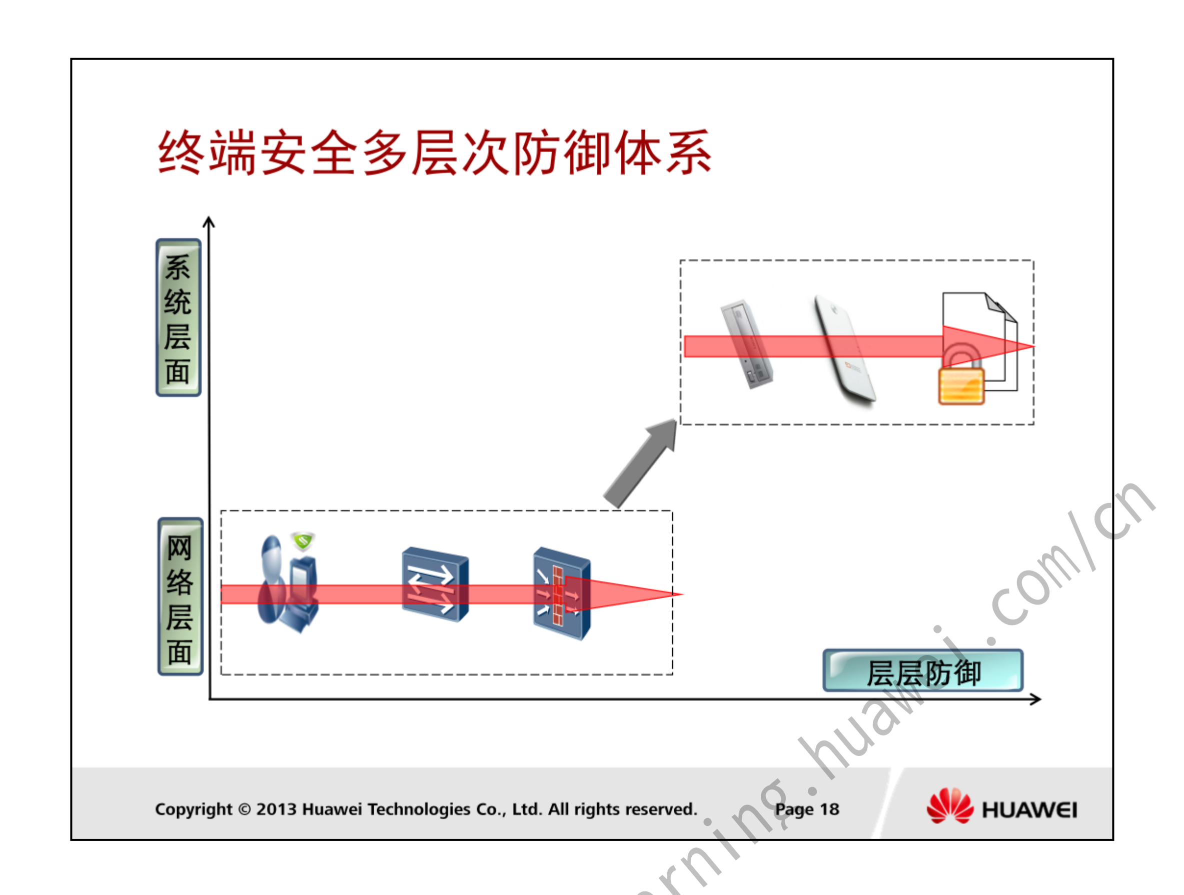
本节主要介绍终端安全系统多层次、全方位防御原理。



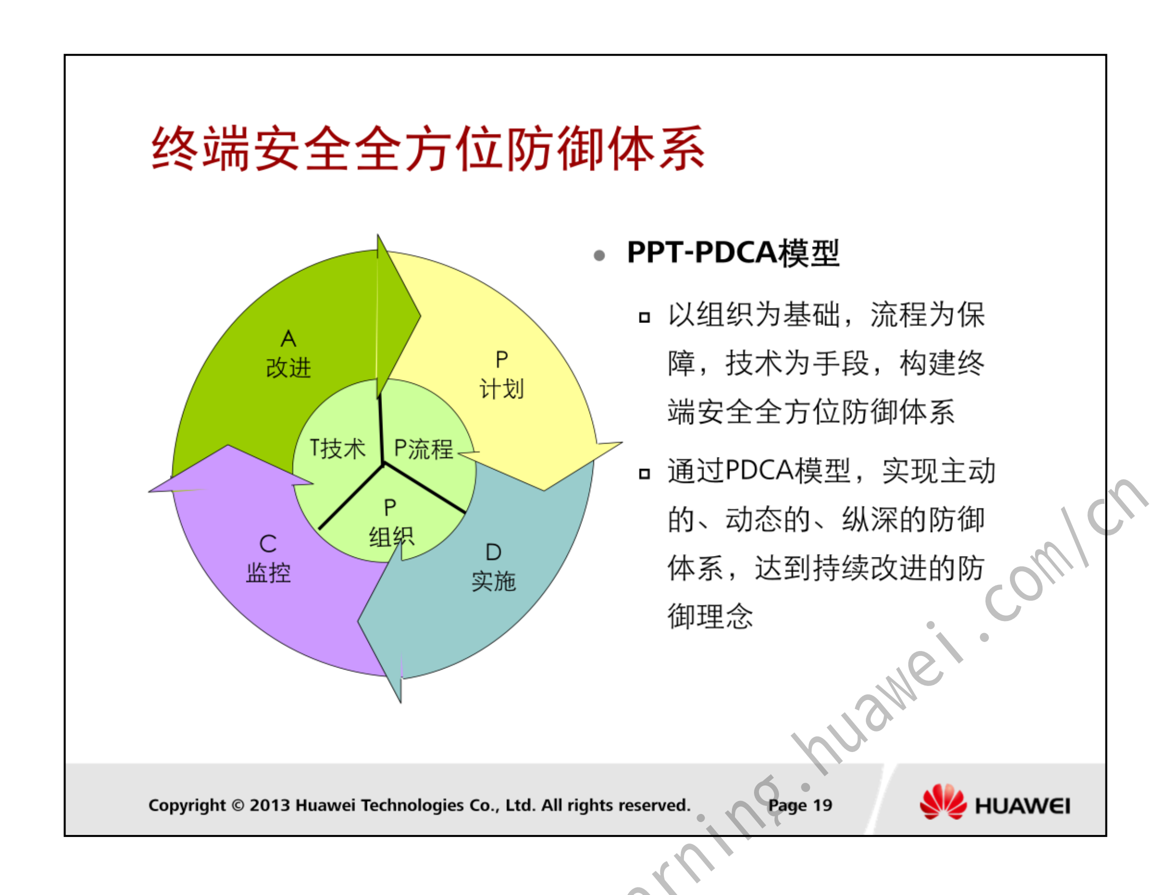
- 立体防御体系，主要体现一体化、多层次、全方位3方面，一体化说明终端安全组件是有机组合，形成统一的整体；多层次说明安全防御是纵深防御，实现终端安全的层层防护，此处不仅体现在网络层面，也体现在系统层面；全方位说明安全是由组织做基础、流程做保障、技术做支撑，也就是以组织做基础，安全管理＋安全技术（安全管理与安全技术2者之间相互相承）。通过构建企业终端安全立休防御体系，保障企业终端实现可管理、可控制、可追溯。



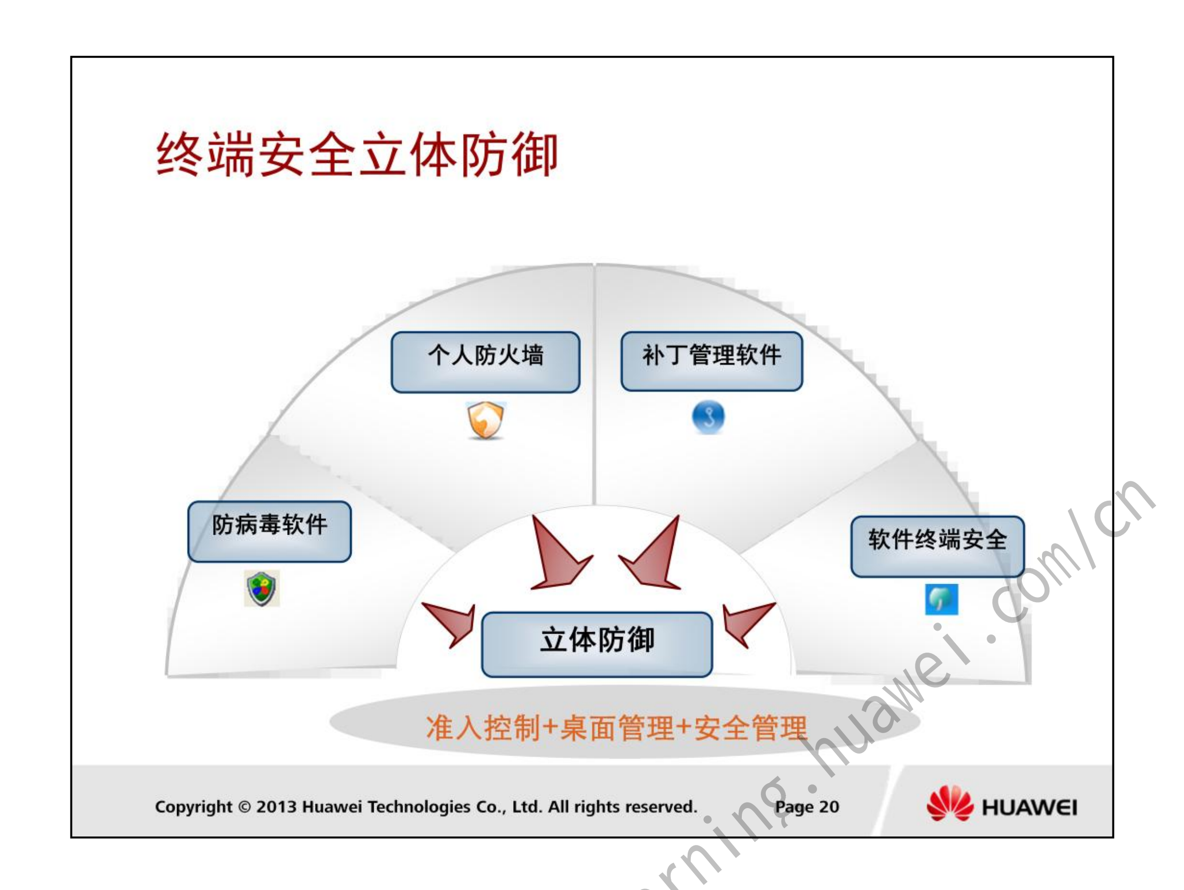
现在我们来看一下终端安全管理解决方案的设计思路。以企业安全策略为核心，用户在接入企业标准网络之前，第一步接受身份验证，认证通过后进行第二步强制合规性检查（包括安全状态和系统配置检查），服务器依据检查结果作出仲裁，符合企业安全策略即可授权访问相应的网络资源；安全检查不合规的终端只能访问修复资源，完成必要的修复后才能接入网络。代理对所有接入网络的终端进行持续的行为监控，及时对违规行为作出响应，并进行记录。整个流程形成了内网安全保护的PDCA持续改进过程。



多层次防御体系，主要体现网络层面和系统层面。网络层面主要通过软件SACG、802.1x交换机、硬件SACG等 3 个层面相互配合，在网络上对终端的接入和业务资源访问进行控制。而系统层面涉及领域比较多，比如对文档资源的访问，可通过封外设端口、控制存储介质、加密文档等措施相结合，对文档的获取进行综合控制，其它象非法外联、病毒防范等也是类似通过综合的控制措施来解决单一措施可能存在的安全风险。这样，通过层层防御最终从根源上降低企业终端可能带来的各类安全风险。



组织，这里是指IT安全业务管理组织和企业业务部门组织；流程，是指信息安全管理制度，及相关法律法规；技术，这里主要指终端安全技术。



什么是终端安全？提到终端安全我们很容易联想到传统的防病毒软件、个人防火墙及补丁管理。从狭义上讲，以上可以是终端安全，但我们也看到，以上终端安全是孤立的，也就是说从广义上来讲，以上部分只能算终端安全组成部分。那么什么是终端安全？终端安全要解决哪些问题？为什么以上传统终端安全产品难以从根本上解决安全所面临的问题？

防病毒软件在20世纪80年代随着病毒产生而产生，经过近几十年的发展，已从当时的个人版发展当前的网络版、网关版。但企业部署完防病毒软件后，发现病毒感染还是大面积发生，虽然有产品自身技术局限性外，其中各终端未按网络管理人员要求进行引擎升级、病毒库升级占大多数，更有甚者某些终端长时间都未安装防病毒软件。而个人防火墙、补丁管理软件在企业部署过程中，也存在与防病毒软件类似的挑战。

基于以上传统终端安全所面临的局限性，21世纪初期，逐步有IT厂商开发出软件类终端安全来解决所面临挑战，但在实施交付中，厂商和企业越来越感到单纯的软件类终端安全很难从体系架构层面来整体解决终端所面临的安全问题。这就促使一批具有综合技术能力的IT厂商介入终端安全领域，华为公司借助自身安全实践、网络技术开发、安全软件开发等能力，提出了终端安全立体防御解决。所谓立体防御，是指基于终端所面临的问题，对相关产品及组件进行整合，形成统一的、整体的纵深防御方案，以解决单一防护可能带来的局限性。

终端安全，是采用立体防御理念形成体系化产品与解决方案。它体现了立体架构和主动防御思想，并通过PDCA来持续提升企业终端的安全能力。终端安全立体防御体系，即通过准入控制来识别终端用户身份，以决定是否允许其接入；桌面管理是通过制定相应安全策略来保障终端桌面的安全；安全管理是通过制定适合企业业务运营要求的安全管理，来确保所制定的安全策略有法可依。



总结

- 什么是终端安全？终端安全有哪些主要特点？
- 终端安全与内网安全有何区别？
- 终端安全在内网安全的位置和地位？





思考题

- 终端主要存在哪些安全威胁?
- 传统终端安全解决方案存在哪些局限性?
- 如何构建终端安全立体防御体系?



练习题

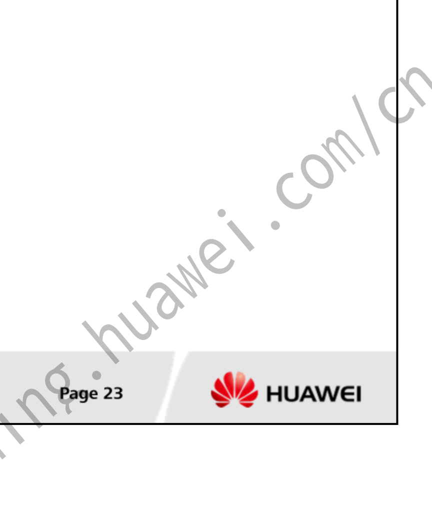
- 判断题
  1. 终端安全不等同于内网安全，因为内网安全包括：终端安全、内部网络安全、业务安全等。
- 多选题
  1. 内网安全包括哪4个区域的安全?

     A.用户域安全

     B.网络域安全

     C.服务域安全

     D.业务域安全



- 习题与答案：
  - 判断题：终端安全不等同于内网安全，因为内网安全包括：终端安全、内部网络安全、业务安全等。

    答案：正确
  - 多选题：内网安全包括哪4个区域的安全?

    A.用户域安全

    B.网络域安全

    C.服务域安全

    D.业务域安全

    答案：A|B|C|D

Thank you

www.huawei.com

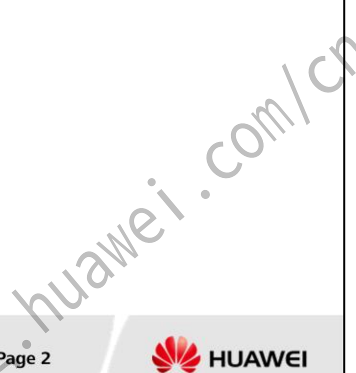
HC120320002
终端安全体系设计

HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解终端安全设计思想；
  - 掌握终端安全相关技术；
  - 了解Policy center的主要功能；
  - 掌握终端安全设计需注意的要素；



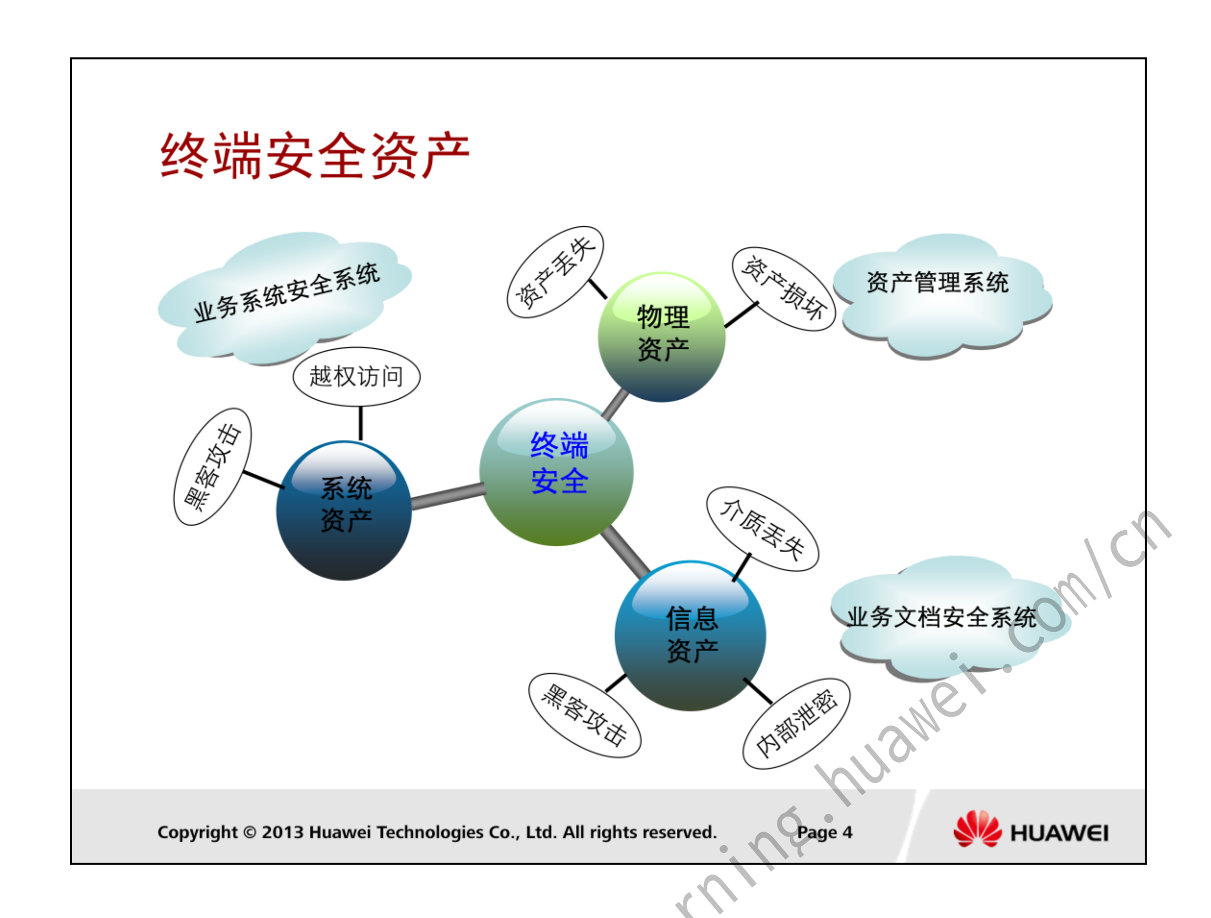
本章介绍了终端安全体系设计思想、相关技术、华为终端安全产品Policy center以及终端安全体系设计方案。

- 重点关注:
  - 终端安全技术
  - 终端安全体系设计方案



目录

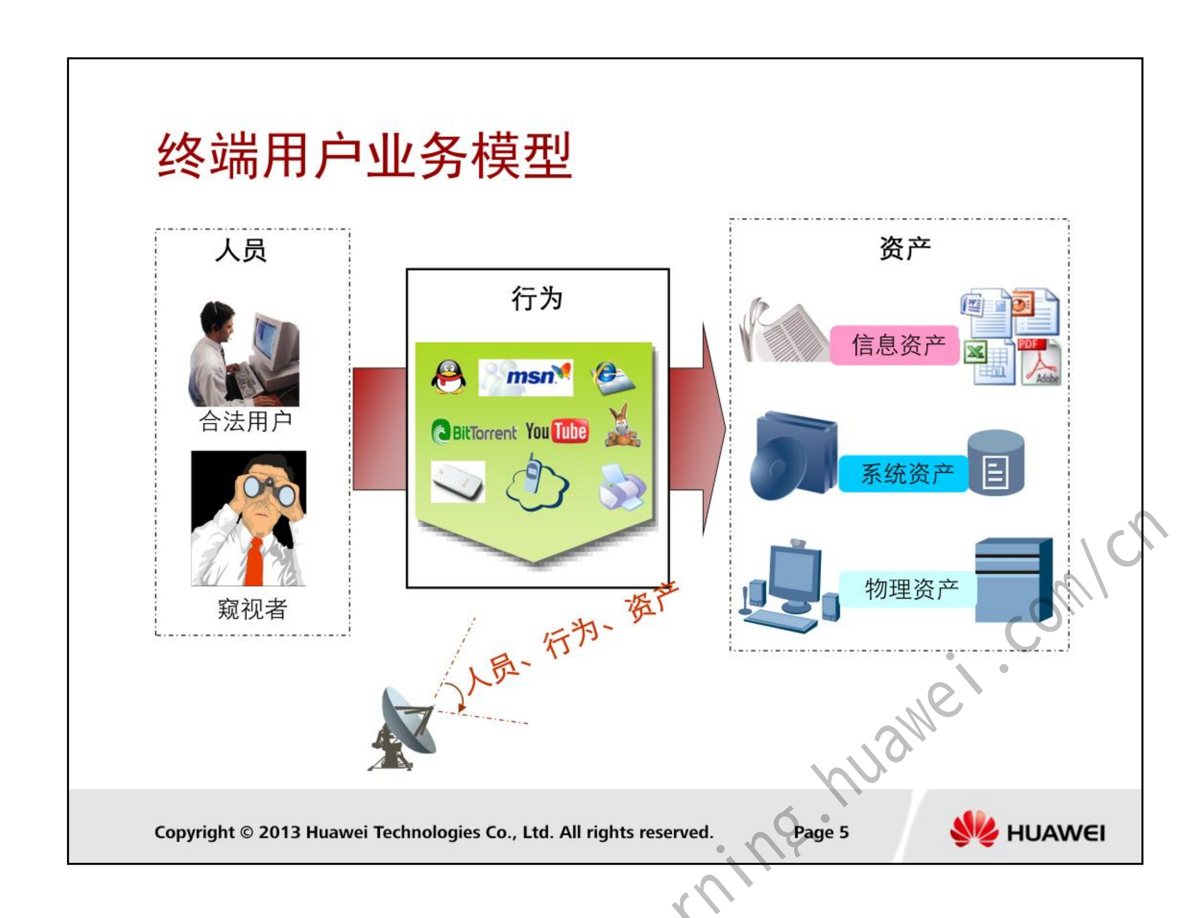
本节主要介绍终端安全体系设计思想，从不同角度分析终端安全设计思路。



讲述终端安全设计思想之前，我们首先要明确我们所保护的目标对象是什么？这样才能从根本上提供对应的防护措施，通过企业的IT安全的分析和多年的业务实践，总结出资产是企业的生命线，是重要保护对象。

资产安全是终端安全立体防御体系所需关注的重要工作，资产主要涉及物理资产、系统资产、信息资产。因3类资产的特殊性，物理资产一般是指终端PC的资产；系统资产，一般是指终端PC的操作系统与应用系统、业务服务器的操作系统与应用系统；而信息资产，一般是指文档信息或数据等信息。

终端安全设计思想是要保障这3类资产的安全，基于这3类资产所面临主要问题的特点，可采用资产管理系统、业务系统安全、业务文档安全系统来解决对应问题。而我们提出的5大要素将对应这3类安全措施，以构建终端安全立体防御体系解决方案。

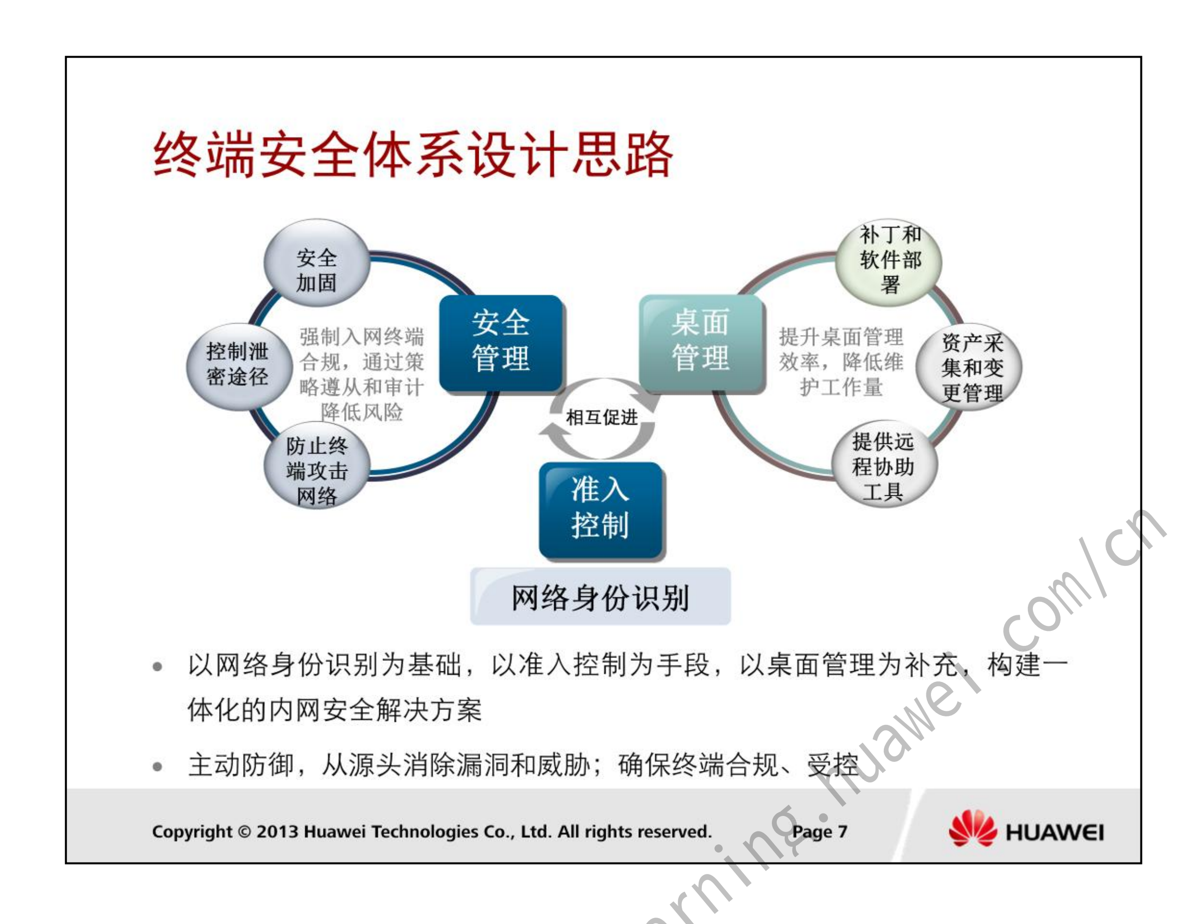


基于终端是内部网络最大的安全隐患源头，是我们在内部网络的控制重点。我们可以对终端用户的业务模型进行分析，可归结于人员、行为、资产，既不同类型人员通过各类行为应用企业的资产。在这应用、使用企业资产过程中，人员和行为均有可能对资产的正常运行造成重大的安全风险。

可能影响资产的安全风险，除了资产自身的系统弱点（操作系统和应用系统所固有的系统缺陷或配置缺陷）或相应的安全措施设置不当外，人员（终端用户）或行为的外在影响将占绝大多数因素。而人员的因素是最难解决、也是最复杂的，由于终端所具有的特点，人员的分类是及其复杂的。比如可分为：内部人员、外部人员；而内部人员根据职位、业务需要，可能分为普遍人员、经理人员、高层人员等，而针对IT管理需要可能也可分为终端用户、管理员、操作员、审计员等；而外部人员根据与企业的业务关系，可能分为客户人员、合作伙伴人员、不相干人员；而内部人员和外部人员若根据安全性来分类，又能分为合法人员、非法人员，且合法人员又能再细分为安全人员、不安全人员。

通过对以上人员按不同维度进行分类，发现他们之间有的属于交集关系，有的则没有任何关系，因此在企业IT组织中，对人员分类是相对困难的也是重要的。由于存在此类现象，那么由人员产生的行为就相对复杂，为了便于描述，可以把人员的行为分为有意行为和无意行为，这两类行为都或多或少对企业的资产造成影响。

有意行为，一般建议采用信息安全流程制度（包括奖惩措施）＋信息安全技术来共同完成，也是本教材重点讲述内容。而无意行为，一般都是被Internet人员通过社会工程等方式利用，此类措施主要是经常给员工进行信息安全意识培训，这类内容不在本教材给予详细描述，请参考相关类型材料。



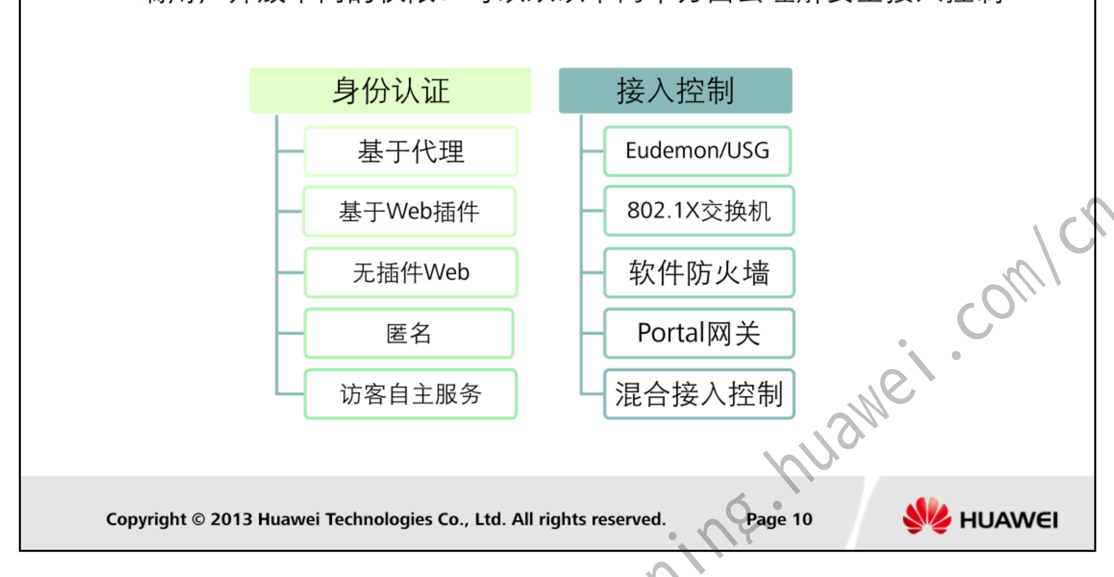
安全管理和桌面管理为相互依存、互为补充的关系，通过桌面管理落实和加强终端安全管理，提高安全管理水平。



目录



- 终端安全技术主要包括以下几个方面：
  - 身份认证：关注身份标识、角色定义、外部认证系统等；
  - 接入控制：关注软件防火墙、802.1X交换机、网关准入控制、ARP、DHCP；
  - 安全认证：关注防病毒软件、补丁管理、非法外联管理、存储介质管理、上网行为管理；
  - 业务审计与授权：关注业务系统权限控制，关注业务系统类审计，各种日志信息，用户操作信息。



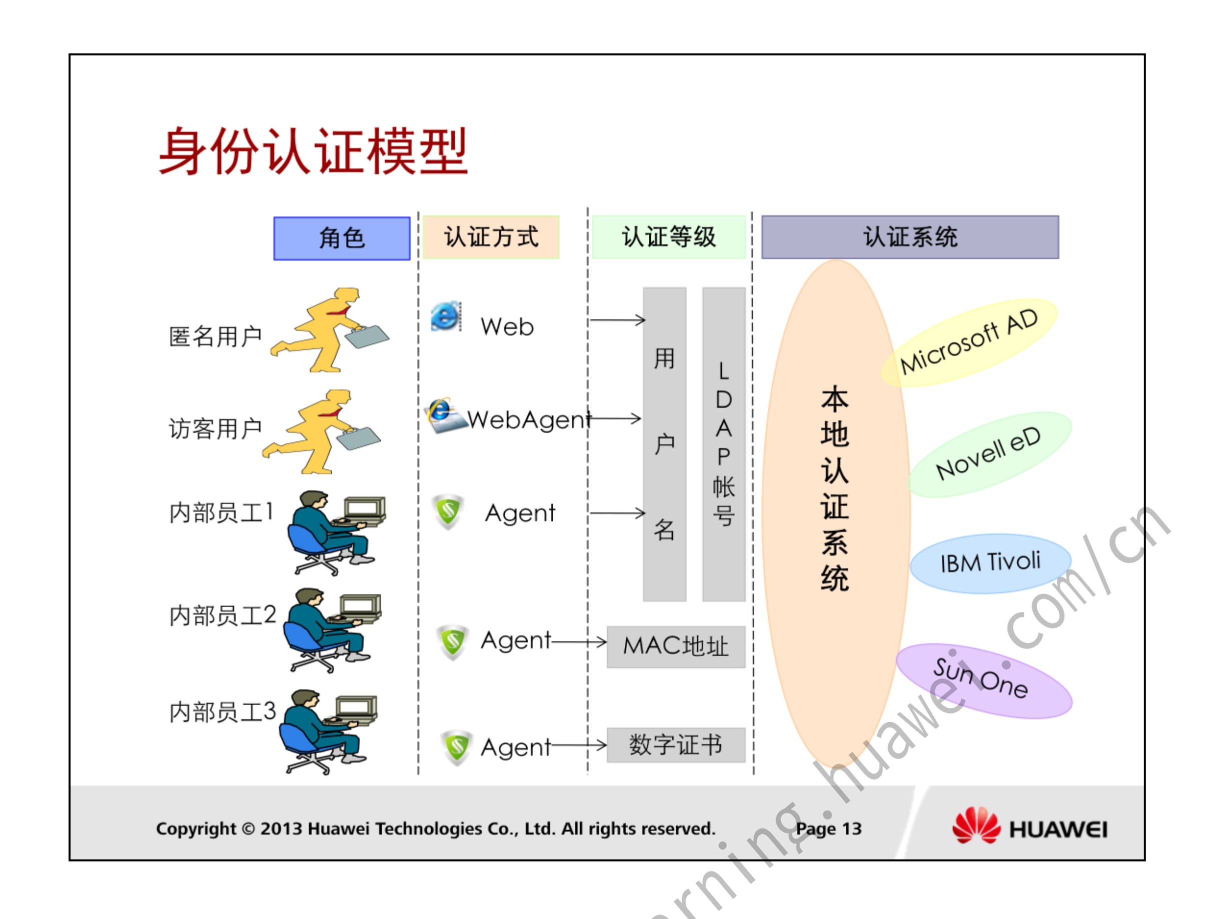
安全接入控制用于控制终端访问网络的权限，对不同安全状况的终端用户开放不同的权限，安全接入主要包括两个方面的内容，身份认证和接入控制，不同的用户角色选用不同的身份认证方式，根据网络环境和网络特点选用不同的接入方式

- 身份认证：
  - 基于代理的认证有普通账号、Microsoft AD域账号、MAC（Media Access Control）账号、第三方LDAP账号多种认证方式。身份认证、执行终端主机安全管理策略和终端用户行为管理策略。其中第三方LDAP包括Novell eDirectory、IBM Tivoli、Sun One等，一般用于企业员工接入认证，需在客户端安装相应终端安全系统的代理软件。
  - 基于Web的认证方式，只要用户登录Web客户端认证界面，身份认证通过后，即可访问正常的网络资源。支持身份认证功能，这种认证方式不需要安装代理软件，方便，但是不利于终端安全管理系统对终端主机的管理，一般不能执行安全策略。一般用于一些临时性的用户。
  - 基于Web插件的认证，不需要专门安装代理软件，可以进行普通账号、Microsoft AD域账号、第三方LDAP账号认证方式。支持身份认证、执行终端主机安全管理策略，但某些辅助工具则不能使用，如远程协助、远程日志采集等。
  - 匿名认证是指终端用户不需要认证账号和密码，在指定的网络区域通过支持匿名认证的登录类型即可完成认证的一种认证方式。对于终端用户，特别是访客，不需要申请特定的账号和密码，使得终端用户能够更容易、方便地通过认证，并接入到受控网络。
  - 支持访客自助服务。 当外来人员需要使用公司的网络时，负责接待的员工提出访客账号申请而不是管理员直接为外来人员申请账号，管理员只负责审批，从而减轻管理员的维护工作量，并由管理器自动记录在案。审核通过后负责接待的员工把账号信息告诉被接待的外来人员，外来人员使用该账号进行身份认证后即可接入受控网络。



目录



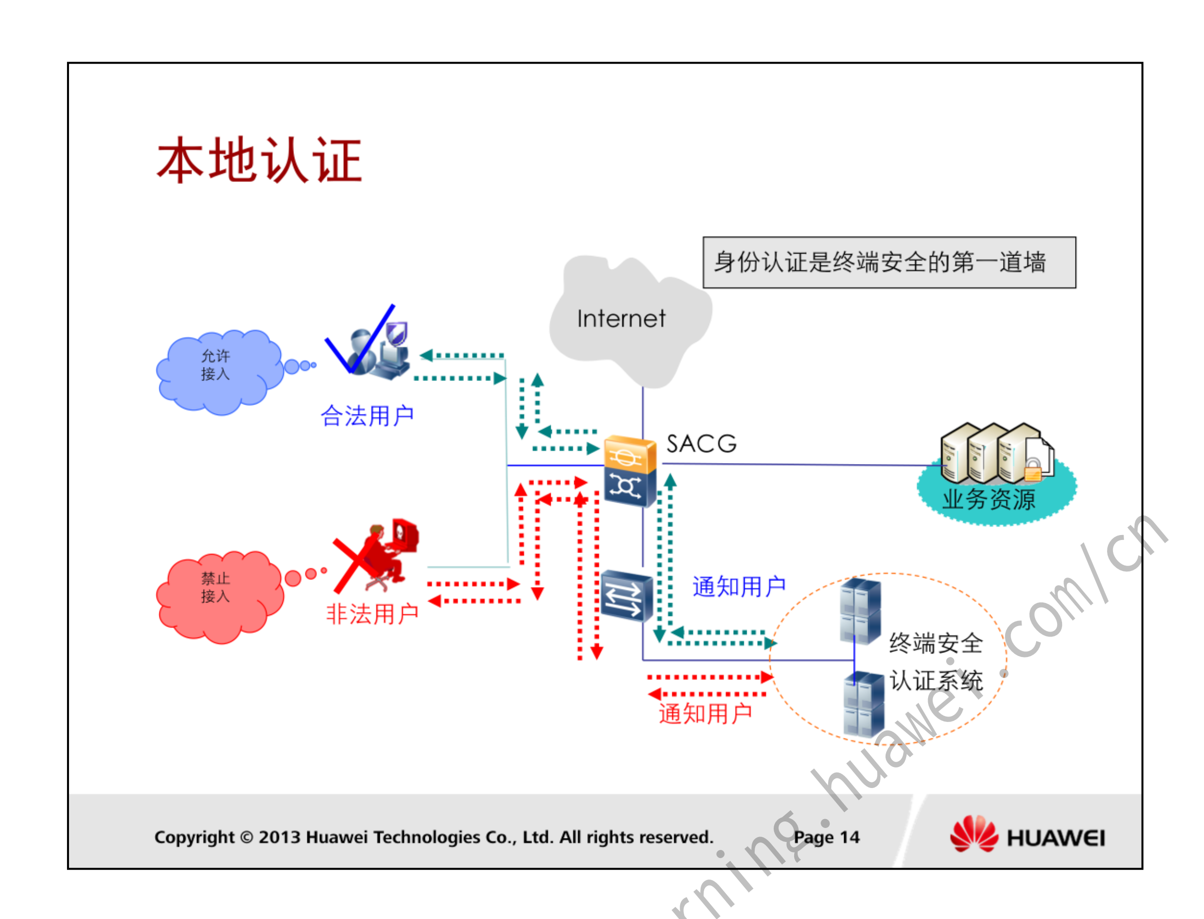


身份认证中涉及几个概念，比较重要的是角色、认证方式、认证等级、认证系统。

角色，既把一组具有业务相关性人员进行的集合。一般在职能型或项目型组织，角色与业务部门或项目组之间有一一对应关系。某一角色可能既属于某一业务部门，又属于另一项目组；认证方式，是终端用户采用的客户端媒介，目前最流行的方式由Web、WebAgent、Agent等3种类型组成。基于Web、WebAgent认证方式在有些功能上可能无法实现，按实现功能强弱来划分从Web、WebAgent、Agent逐步提升，既Web功能最弱，Agent功能最强；认证等级，一般有2种等级，一种等级为我知道、我拥有、我具有，而另一种等级为单因素、双因素、多因素，不管哪种方式，最重要是关注安全强度和投入成本之间的平衡；认证系统，是身份认证的数据源，一般情况下终端安全软件自身带了认证系统，或可与企业自身的认证系统进行整合，目前业界流行的认证系统主要是LDAP。

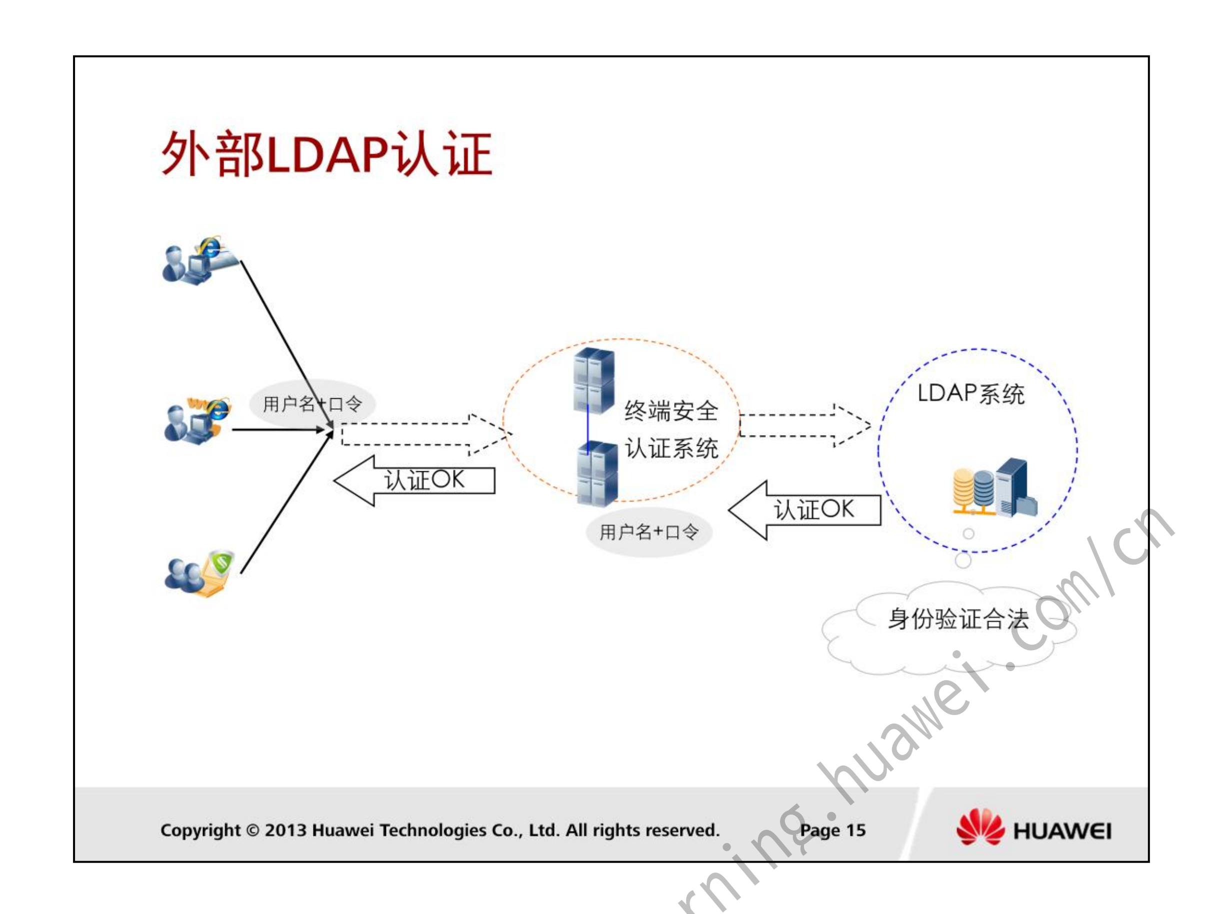
华为终端安全系统，提供三种方式进行身份认证，包括web客户端、web客户端插件、客户端agent等；提供的五种身份认证类型包括：普通账号认证、AD域账号认证、MAC账号认证、LDAP账号认证、数字证书认证。其中web客户端、web客户端插件可支持普通账号、AD域账号、LDAP账号三种进行认证，agent可支持上面全部五种类型。

LDAP（Lightweight Directory Access Protocol）：轻型目录访问协议，是指能够使用LDAP协议存取数据的目录服务。LDAP目录以目录树方式呈现自身存储的数据，它由若干种对象组成，允许管理员给出若干个对象的属性快速定位至该对象，具有较好的搜索性能。LDAP目录通过账号和密码来验证终端用户身份的合法性。华为终端安全产品支持与Novell eDirectory、Microsoft AD域控制器、IBM Tivoli、Sun One、JIT Galaxy及按照标准LDAP协议实现的目录服务器联动来完成终端用户的身份认证。



身份认证作为内网安全的基础，是终端安全的第一道墙，通过身份认证可以拒绝非法用户对内网资源的使用或者破坏。通过本过程，对用户的身份进行标识，为后续业务授权、监控、审计等提供身份标识。

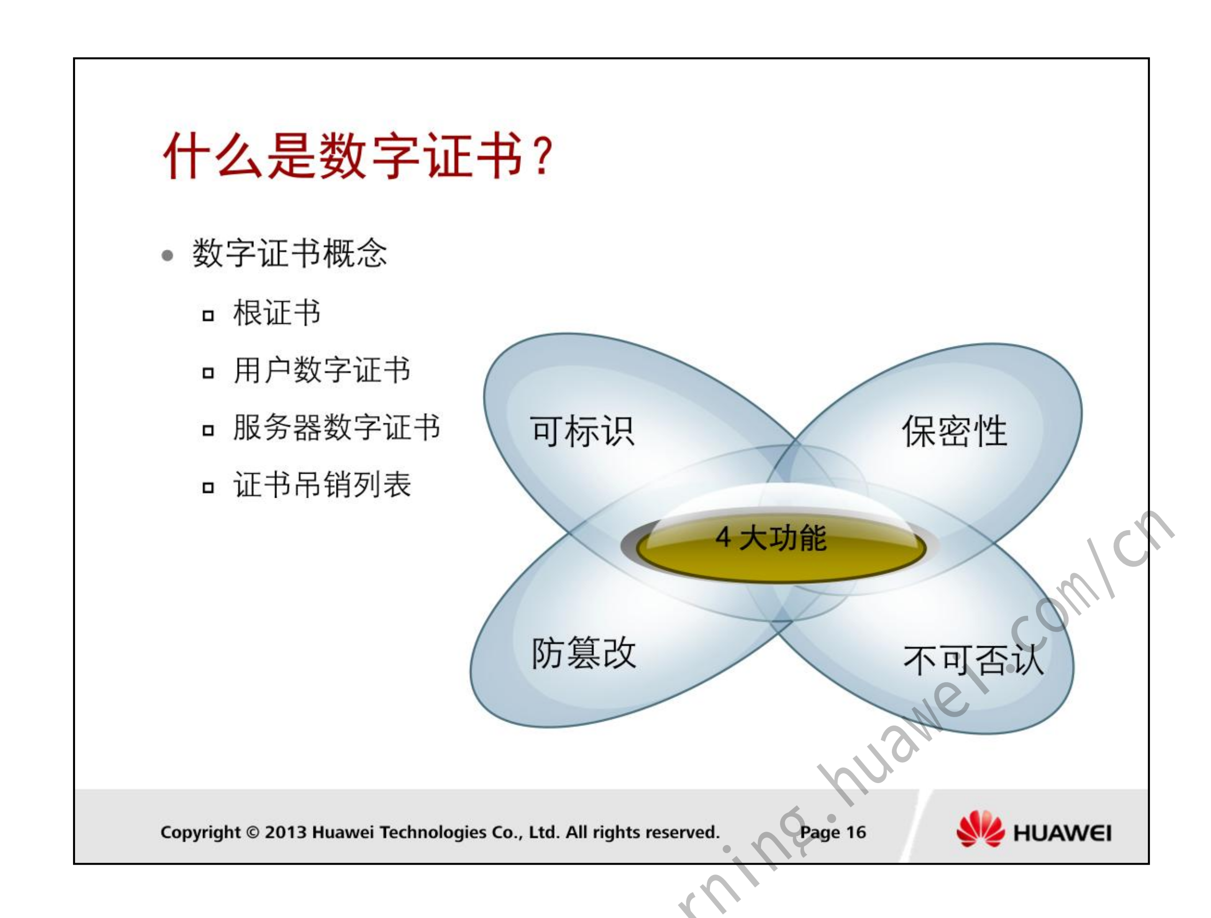
本地认证，即用户的身份标识信息存储在终端安全系统的数据库，在身份认证时，客户端与终端安全系统交互信息，以验证客户端的合法性。



终端安全体系除了支持本地认证系统外，还支持与外部LDAP认证系统进行整合，以降低企业投资与日常运维复杂性。采用外部LDAP认证系统后，用户帐号的合法性将由其来验证，在接收到由原来终端安全认证系统传递过来的用户信息，外部LDAP将接收到的用户名与口令信息进行验证，若通过将向终端安全认证系统返回确认信息，证明此用户帐号为合法。

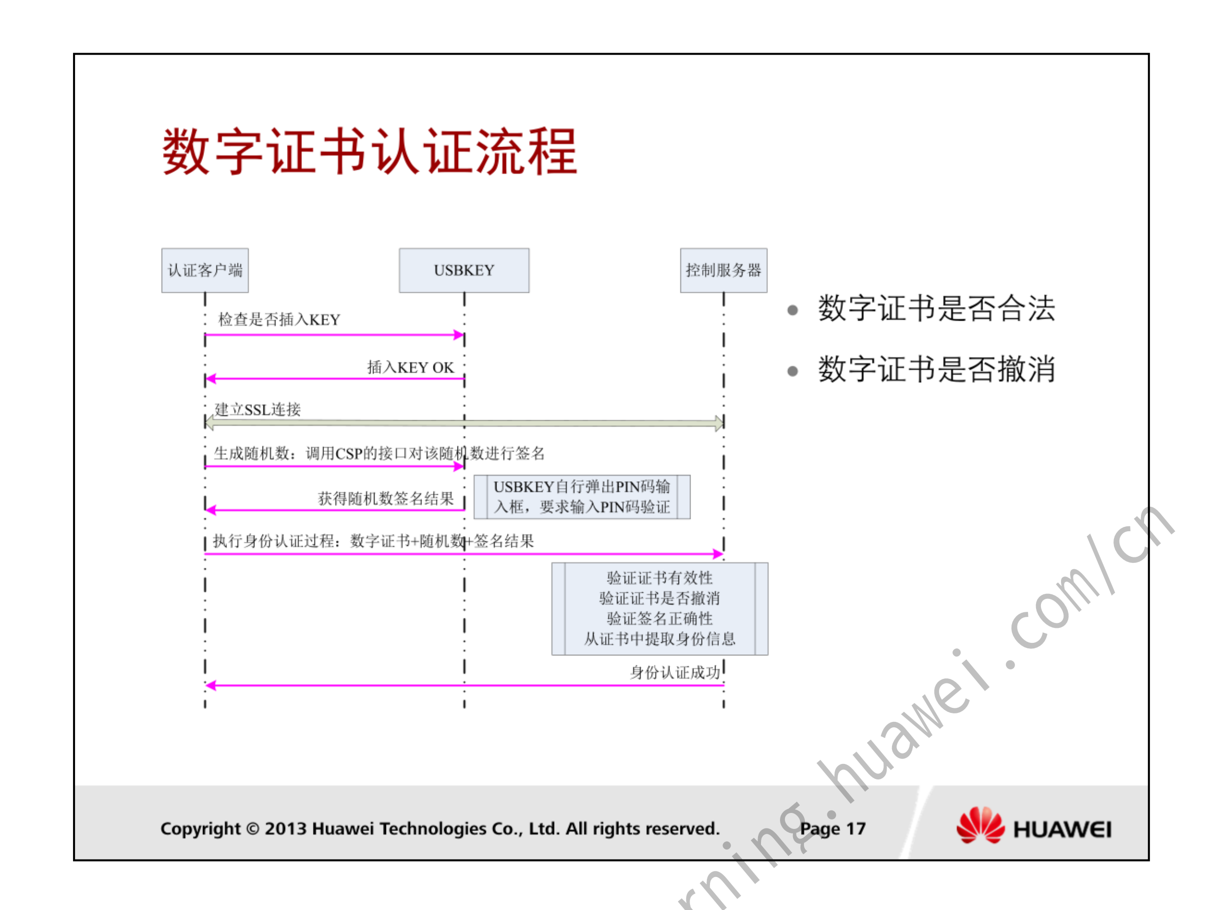
终端安全系统可以支持若干个外部数据源，具体依据不同产品及版本而定，同时可以支持配置主备外部认证源，增强可靠性。

此认证方式可支持Web、WebAgent、 Agent 3种类型。



在终端安全立体防御体系中，加入数字证书认证方式可加强身份认证的级别。它主要由4大功能组成：可标识，唯一标识用户身份；保密性，数据传输过程不会泄密；不可否认，操作过程不可否认；防篡改，数据传输过程不被篡改；

- 数字证书主要涉及以下概念：根证书、用户数字证书、服务器数字证书、证书吊销列表。
  - 数字证书：由用户信息、用户公钥、签名信息等3部分组成；
  - 根证书：由CA认证中心给企业颁发的数字证书，其是证书体系中最特殊的一种证书，它的签发者是它自身，也既是其它数字证书的基础；
  - 用户数字证书：用来证明用户合法身份的一类数字证书，其使用根证书进行签名；
  - 服务器数字证书：用户证明服务器合法身份的一类数字证书，其使用根证书进行签名；
  - 证书吊销列表：由CA认证中心签署的一系列失效数字证书列表，数字证书均有一定的生命周期，但因业务原因需缩短其生命周期。



- 关于USBKEY的PIN码问题
  - 是否需要弹出PIN码输入框，以及如何弹出，均由USBKEY产品自身实现，与后台服务器无关。
- 关注用户身份信息提取
  - 证书如何映射到账号，需要在服务器端配置。
- 支持USBKEY认证
  - 原则上，只要USBKEY支持标准的CSP接口都能够支持。建议以测试的情况为准，因为不同厂商实现的情况还是有一些差异，具体已验证厂商请查找相关产品文档确认。



目录



接入控制技术



软件SACG：

可有效控制局域网内终端主机互相访问的行为。

对业务系统防护能力较差



802.1X交换机：

对设备的整体性能要求不高，可有效降低建网成本。

配置和维护802.1x交换机过于复杂，在出现故障时必须手动关闭802.1x。



Portal网关：

基于动态VLAN、动态ACL下发的用户角色访问

只适用于规模较小的网络，终端较集中的场景



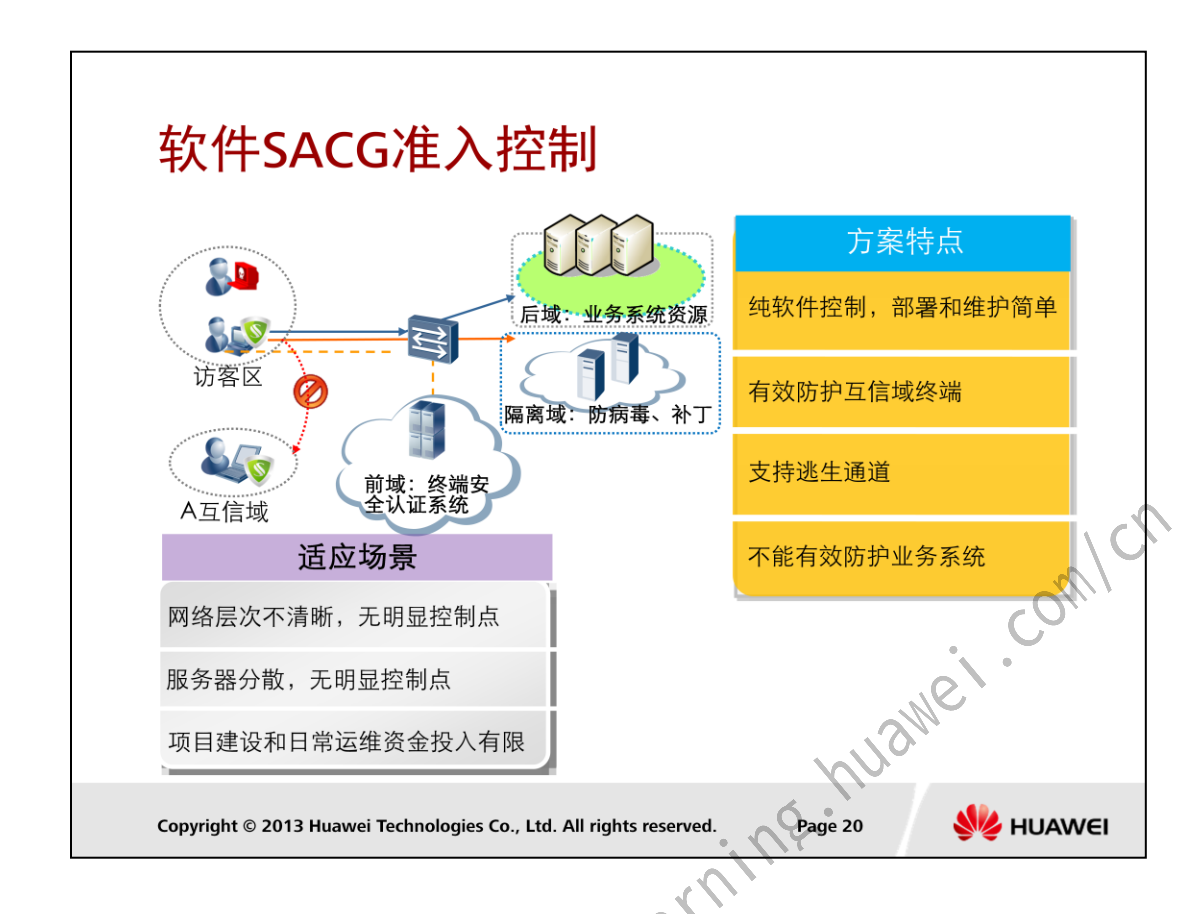
硬件SACG：

适用于各种规模的网络，基于角色进行访问控制

终端之间的访问不能有效的控制



- 软件SACG/终端互访控制：是内置在终端Agent上的一个组件；
- 标准802.1X交换机：支持业界流行802.1X交换机，如华为、H3C、CISCO；
- PORTAL网关：华为交换机的3300\5300系列交换机（软件版本V100R006），能够作为PORTAL网关，实施准入控制；
- 硬件SACG：终端安全系统可以与全系列华为中低端防火墙联动（如USG系统）。

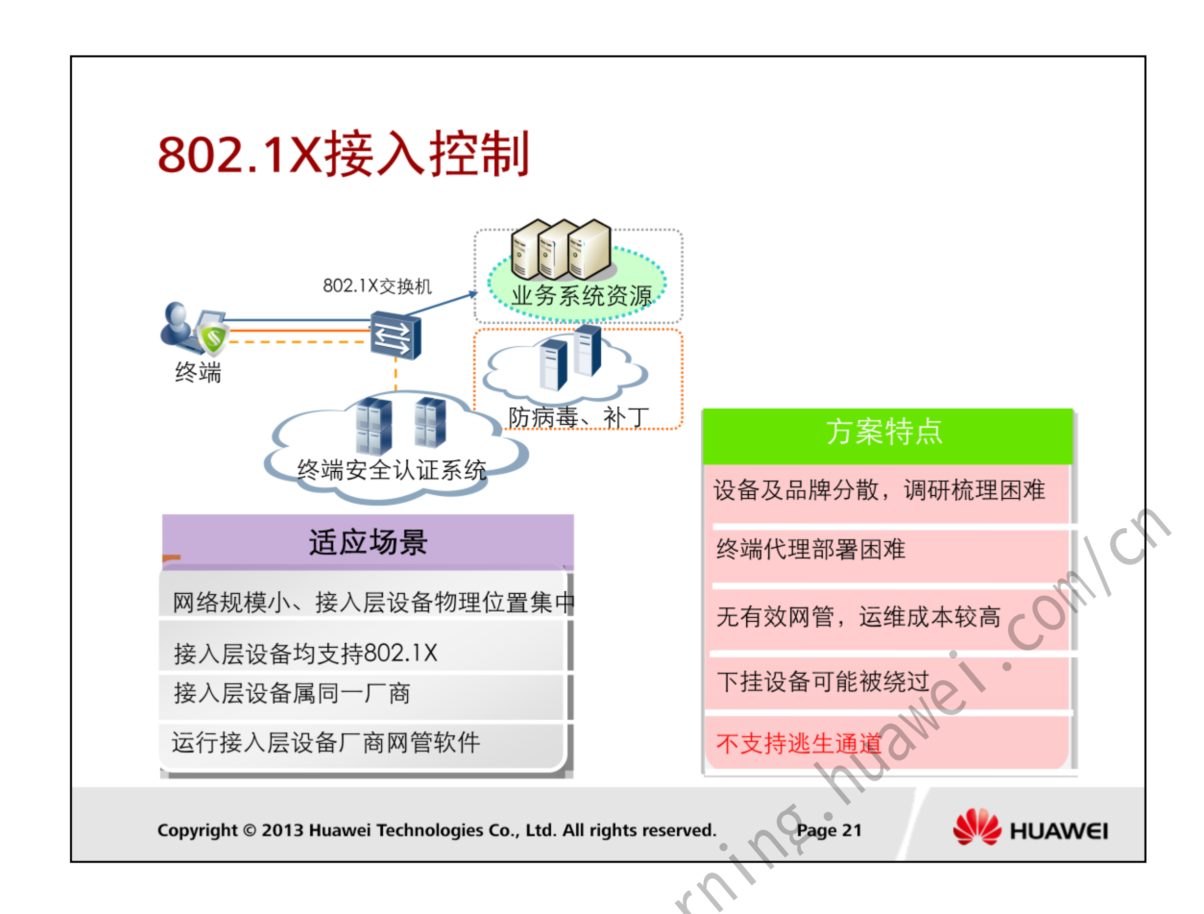


软件SACG准入控制方式是纯软件类方案，其最大特点是部署灵活、维护简单，可有效地防护区域终端的安全，但不能很好地对业务系统进行防护，但其可通过与802.1x准入控制或网关级准入控制技术进行组织，实现终端之间和终端与业务系统之间双重安全防护。

此类准入控制方式比较适应以下场景：1)网络层次不清晰，无明显控制点；2)服务器分散，无明显控制点；3)项目建设和日常运维资金投入有限的企业环境。此方案最大的缺点是无法有效地对企业业务系统进行防护。

在终端安全系统的组成部件中并不存在软件安全接入控制网关这个软件实体。通过管理员在终端安全管理器上配置的规则并下发至代理执行来控制终端主机接入受控网络。所以是终端安全管理系统和终端代理共同完成接入控制，所以软件的SACG接入控制方式的接入客户端需要代理。

- 安全域：
  - 认证前域：终端安全认证系统。
  - 认证后域：企业业务系统。
  - 隔离域：防病毒、补丁等各种修复服务器。



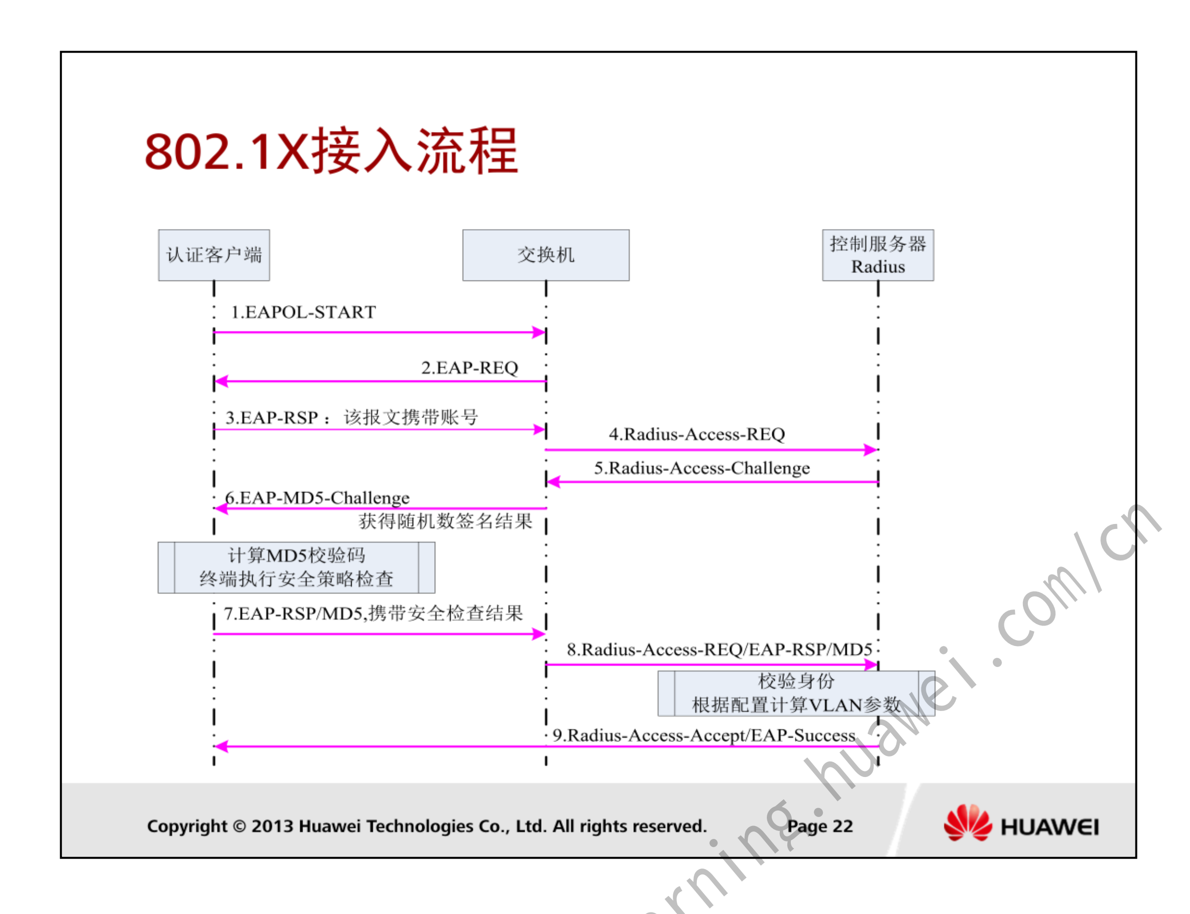
讲述802.1X准入控制前，我们先了解一下基于端口的802.1X协议起源， 制订802.1X协议的初衷是为了解决无线局域网用户的接入认证问题。在它的设计体系结构中采用了“可控端口”和“不可控端口”的逻辑端口，实现认证流和业务流的分离，既由认证系统和802.1X交换机利用不可控的逻辑端口共同完成对用户的身份进行认证，使其由不可控制端口转变为可控端口后，完成业务流数据的传输。

基于标准802.1X准入控制方式，此最大特点是：1）网络内设备及其品牌多样化，存在调研困难，可能导致代理部署困难，运维成本较高。若运行了接入层设备厂商网管软件可能可以降低运维成本，比如交换机出现故障，可能需人为至现场进行手工修改；2)由于实现了身份认证与安全认证的分离，再加上802.1X固有的准入能力，使其准入控制能力特别强，但由于单纯的标准802.1X无法把安全认证进行整合，致使其安全认证控制能力特别弱，既无法实现对不安全终端的隔离修复；3)可能存在终端用户私自下挂设备，导致可能被绕过现象，华为设备可通过基于MAC地址认证来解决，其它厂商设备可能存在此现象。

下挂设备若为智能HUB或低端交换机（需支持组播透传），可能存在802.1X认证报文无法穿越问题。

介于以上特点，标准802.1X准入控制适应场景为：1)网络规模相对比较小，且接入层设备物理上比较集中环境；2）接入层设备均需支持802.1X，且属于同一厂商设备；3）最好有运行接入层设备厂商的网管软件。

若单纯从准入控制角度，802.1X是个不错的解决方案，除了部署复杂些和无法实现逃生通道外。



- 有线802.1X终端与交换机之间交互EAP报文，交换机与服务器之交互Radius报文，基本认证流程：
  1. 终端AGENT通过发送EAPOL-START，触发交换机发起802.1X认证流程
  2. 交换机发送EAP-Request/Identity，对触发报文进行回应开始802.1X的认证流程
  3. AGENT发送EAP-Response/Identity消息，该消息携带终端的账号信息
  4. 交换机收到EAP-Response/Identity消息，把该消息封装成Radius报文，发送给Policy Center服务器（ Policy Center服务器提供Radius服务）
  5. Policy Center服务器决定使用MD5的方式进行认证，使用Radius协议封装EAP-Request/MD5-Challenge消息，发送给交换机；
  6. 交换机转发EAP-Request/MD5-Challenge给终端AGENT
  7. AGENT计算MD5值，根据离线策略做安全检查，把MD5值和安全检查结果，通过EAP-Response/MD5，发送给交换机
  8. 交换机通过Radius封装，转发EAP-Response/MD5
  9. 服务器收到该EAP-Response/MD5后，首先检查身份是否OK，然后检查安全检查结果，根据安全检查结果/以及系统配置，决定是否发送VLAN参数
  10. 当代理收到EAP-SUCCESS的消息，确认802.1X认证通过,这时候Policy Center AGENT会检查终端的IP地址获取方式，如果是使用DHCP获取IP地址，则触发获取IP地址。

MAC旁路认证和无线802.1X

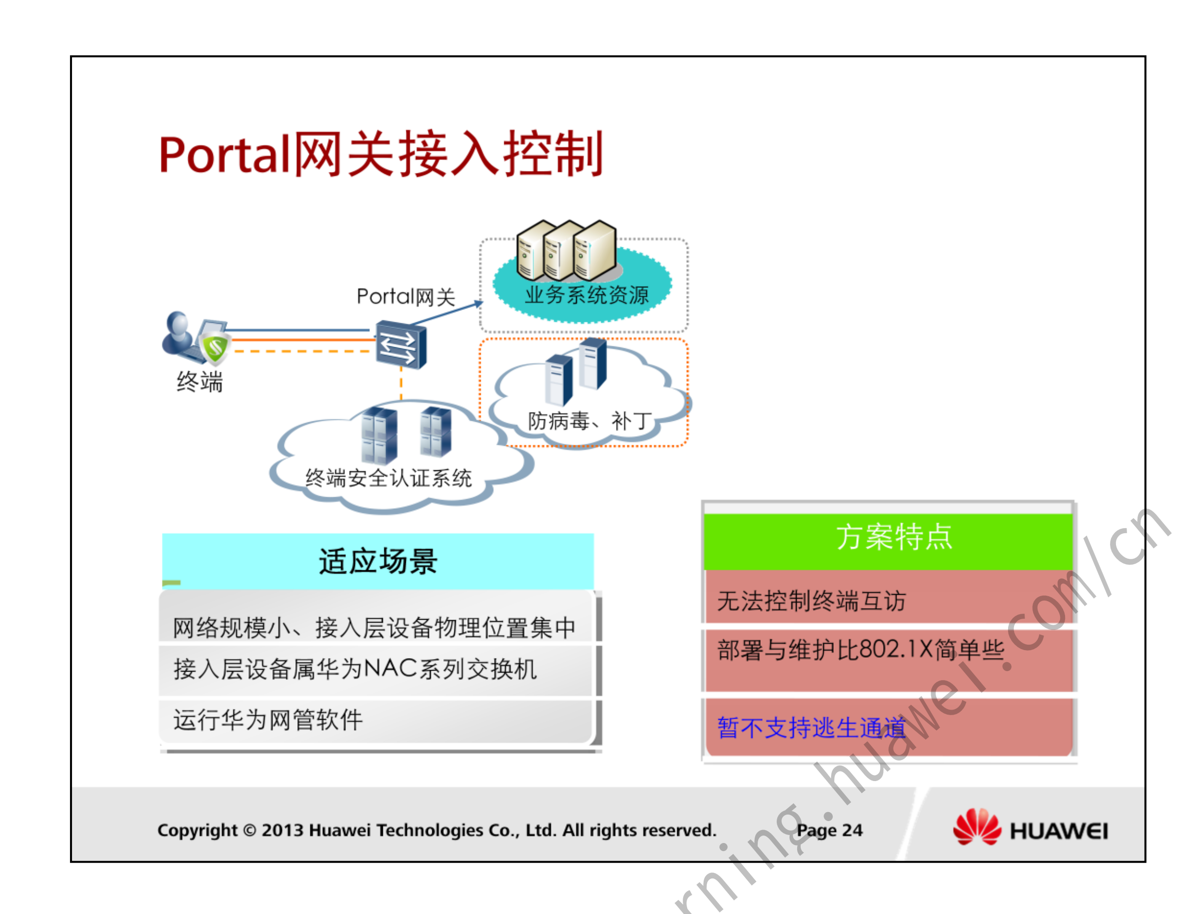
- 在日常场景中，有很多许接入受控网络的设备是不能安装终端代理的，如打印机，IP 电话等，还有一些设备可能安装的是非华为802.1X终端，针对以上两种场景，我们应对方法有：

MAC旁路认证	• 打印机、IP电话、传真机、业务服务器等
增加无线网络的SSID	• 智能设备，Windows 802.1X客户端，其他第三方标准客户端。



当启用802.1x交换机接入控制方式时，只有通过NAC Agent客户端完成认证的设备才能正常访问网络，即终端必须安装代理，对于打印机、IP电话等设备，由于不能安装和使用NAC Agent客户端，为了保证这些设备能够正常访问网络，需要将这些设备添加为MAC旁路认证设备。由于MAC旁路认证设备具有访问整个网络的权限，请妥善添加MAC旁路认证设备

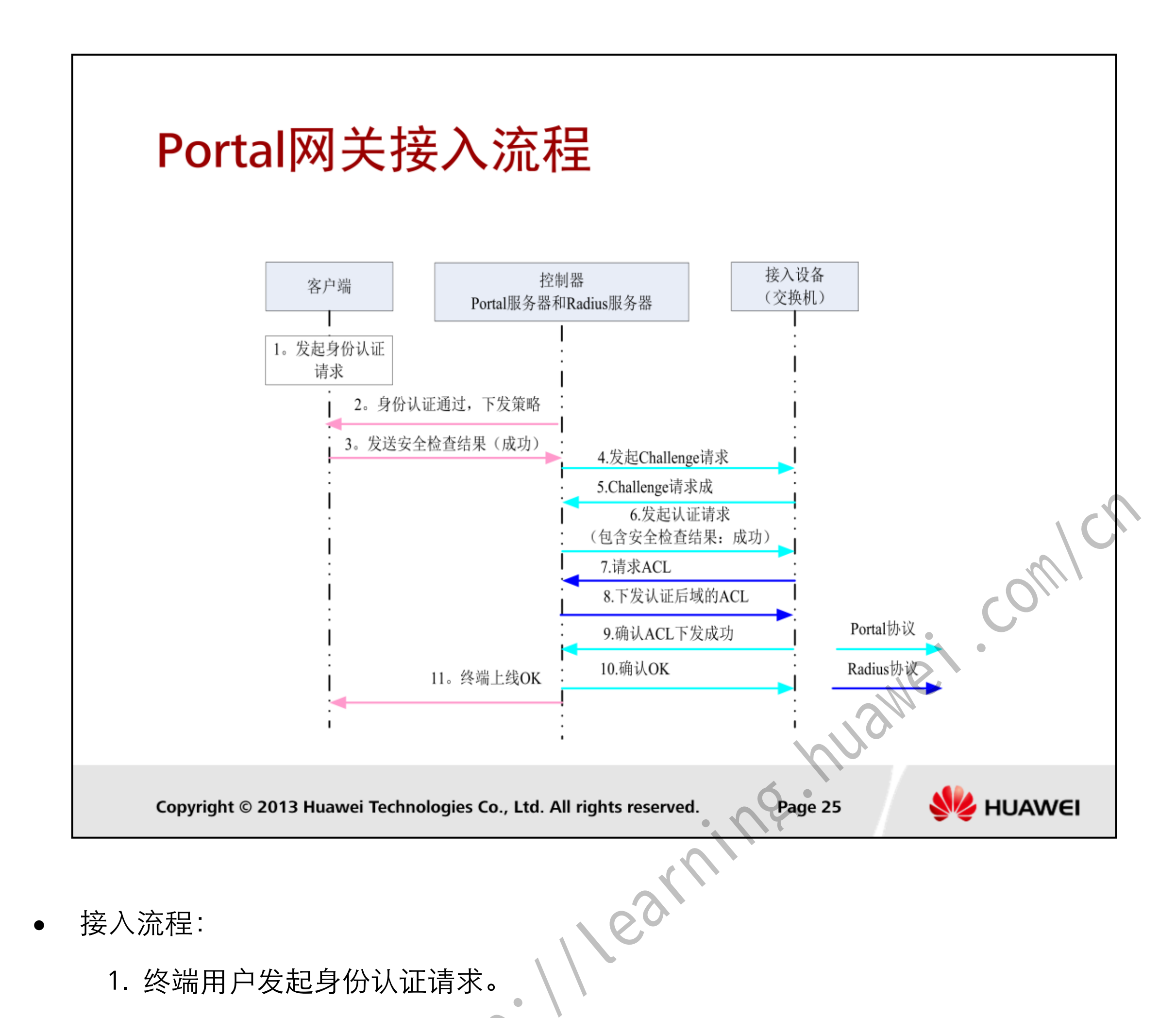
对于没有安装代理的终端设备，如果需要使用其他的802.1X客户端向管理器认证以接入无线网络，则需要将这些设备所连接的无线网络SSID配置到管理器的SSID列表中。使用其他802.1X客户端的终端设备包括：智能设备、Windows操作系统自带的802.1X客户端以及其他支持标准协议的第三方802.1X客户端。



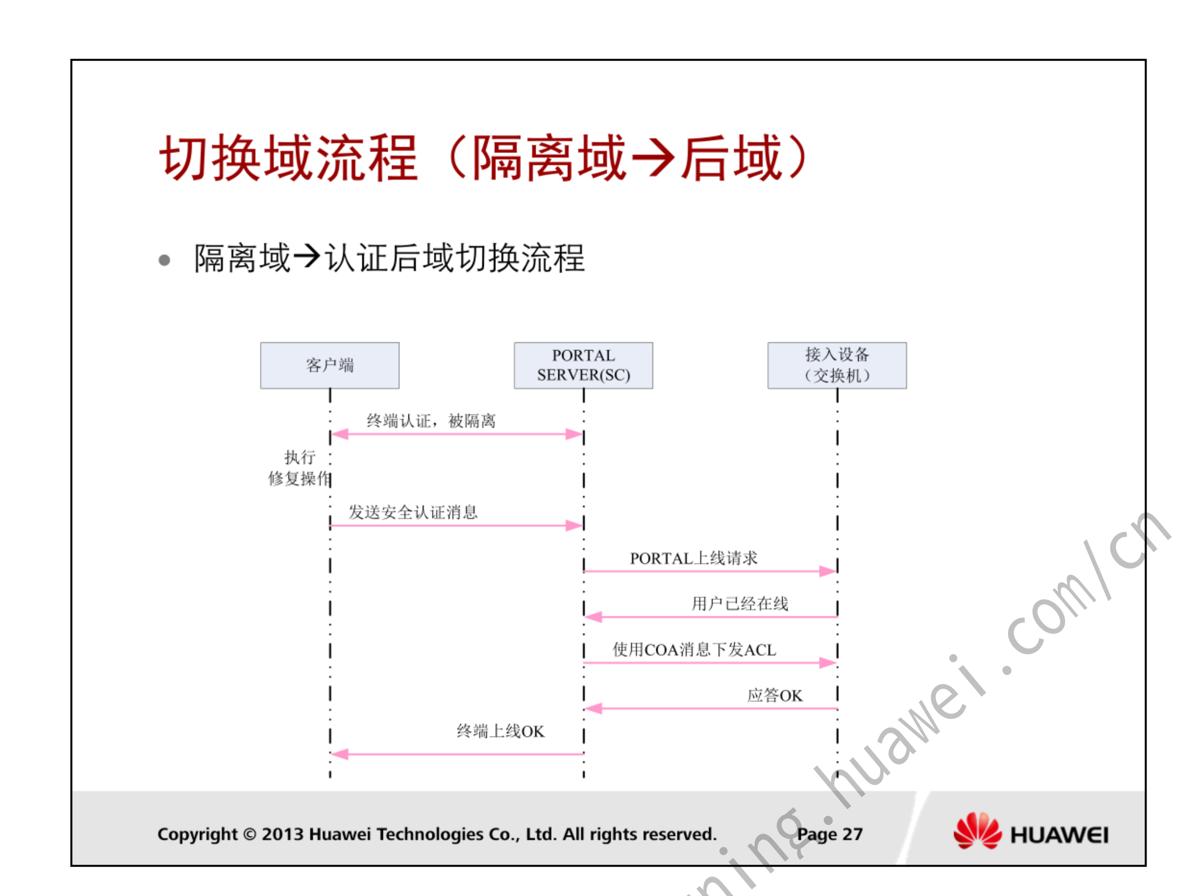
Portal网关准入控制技术，采用Portal认证对终端用户进行身份认证或身份认证和安全认证。Portal认证也称Web认证，其基本原理是：终端用户首次打开Web浏览器，访问任何网址，都被强制重定向到Portal服务器的认证页面。只有在身份认证通过后，终端用户才能访问网络资源。未认证的终端用户只能访问特定的站点服务器。Portal认证通过Web页面输入用户名和密码，使用Portal协议完成认证过程。但为了完成安全检查任务，终端主机必须安装终端代理或Web Agent插件。

采用802.1x控制方式或PPPoE控制方式控制终端主机接入受控网络，只可对接入层的终端用户进行控制，并且必须在终端主机上安装客户端，组网方式不够灵活。而Portal认证控制方式具有上述两种控制方式不具备的优势，一方面Portal网关部署在接入层或数据中心的出口处，部署位置灵活，另一方面终端主机无须安装客户端，降低部署成本。

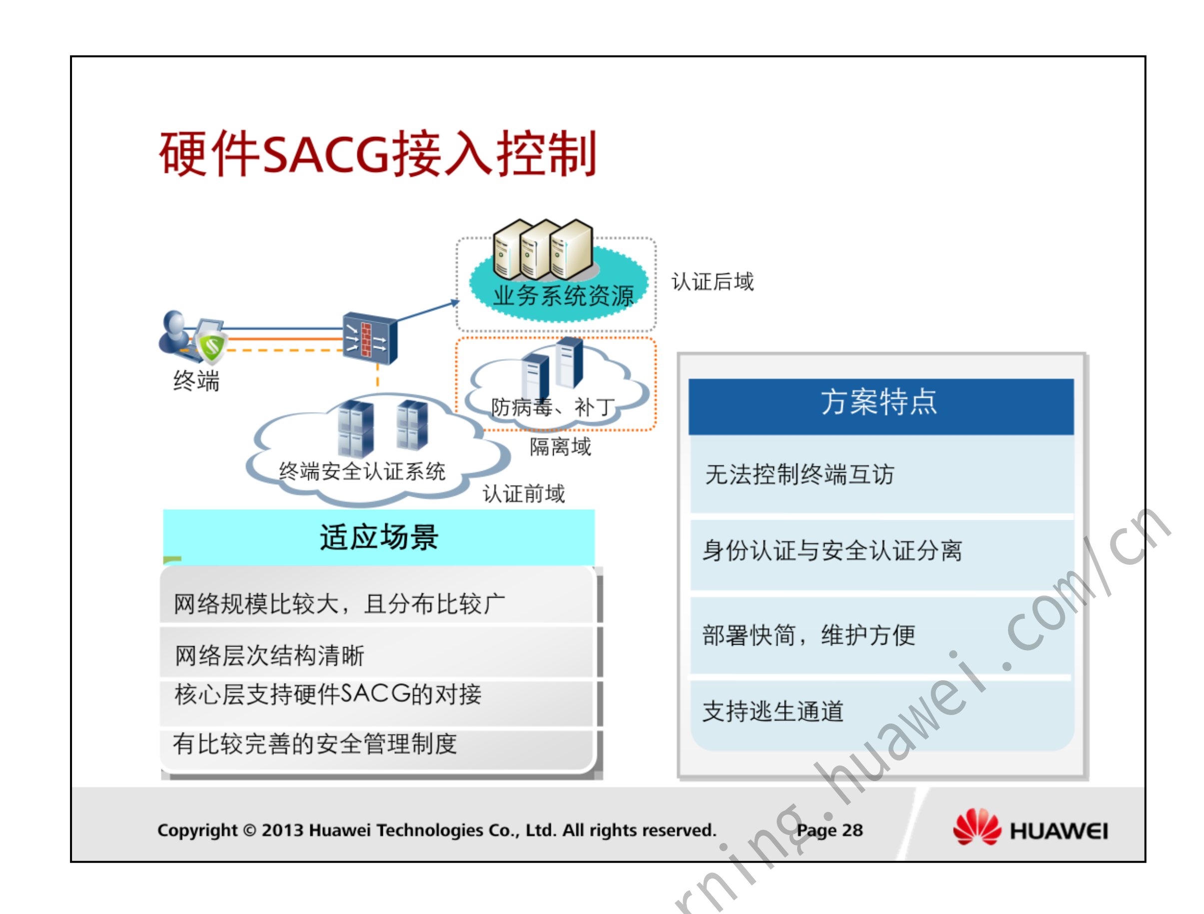
Portal网关准入控制目前还暂不支持逃生通道机制。



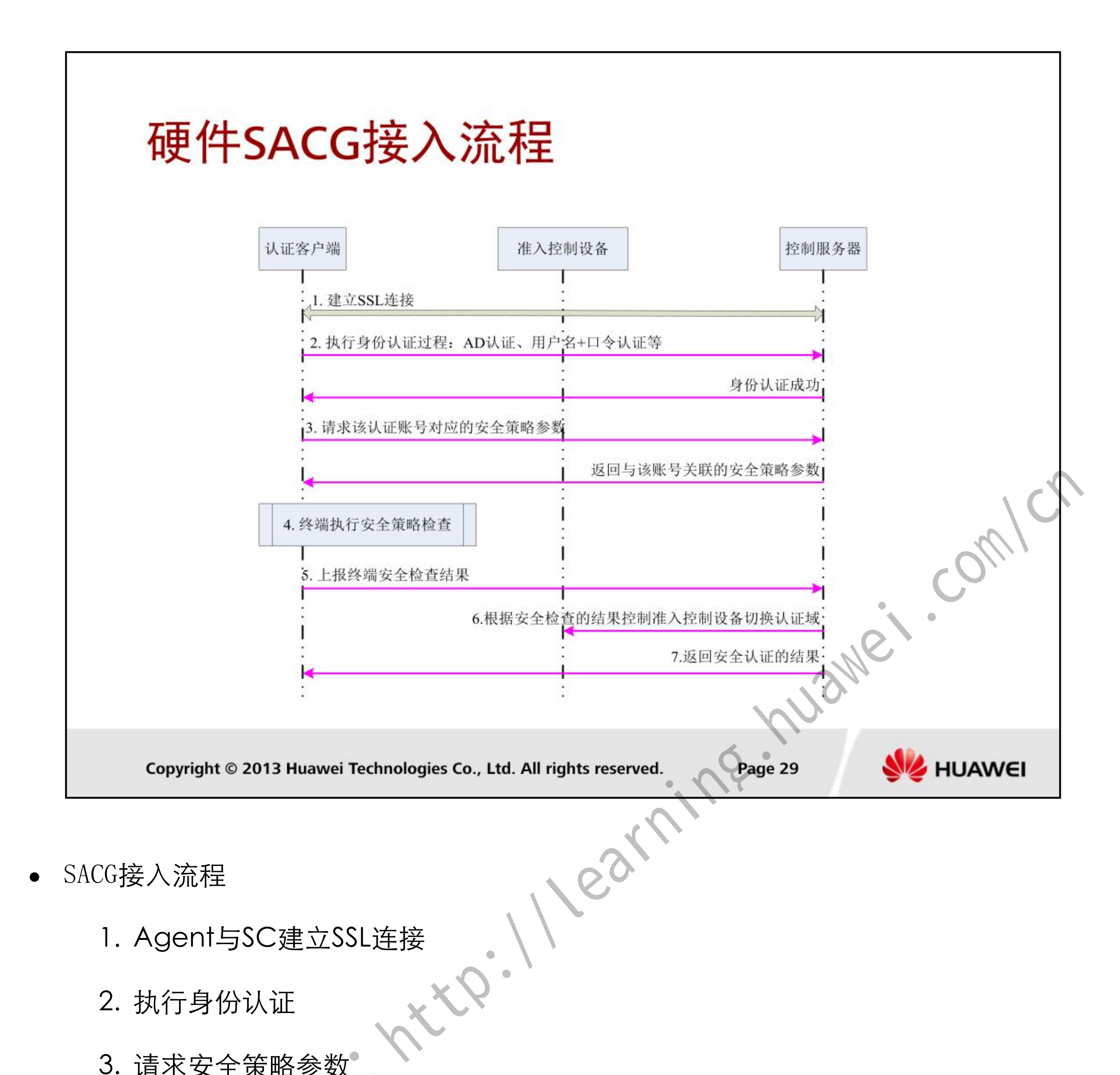
- 接入流程：
  1. 终端用户发起身份认证请求。
  2. 在终端用户通过身份认证后，控制器向代理或Web Agent插件下发策略。
  3. 代理或Web Agent插件执行策略，然后向控制器发送安全检查的执行结果（认证通过）。
  4. 这里属于Portal认证流程的起点，控制器（角色是Portal服务器）向交换机发送Challenge请求报文，同时开始计时，等待交换机的应答。如果在指定的时间范围内没有收到来自交换机的应答，则重新向交换机发送Challenge请求报文。如果达到最大发送次数依然没有收到交换机的响应，则通知代理或Web Agent插件认证失败。
  5. 交换机发送Challenge应答报文。
  6. 控制器（角色是Portal服务器）按CHAP算法计算CHAP-PASSWORD，在扩展字段附加安全检查结果（安全检查通过），然后向交换机发起认证请求，同时开始计时，等待交换机的应答。如果在指定的时间范围内没有收到来自交换机的应答，则重新向交换机发送请求报文。如果达到最大发送次数依然没有收到交换机的响应，则通知代理或Web Agent插件认证失败。



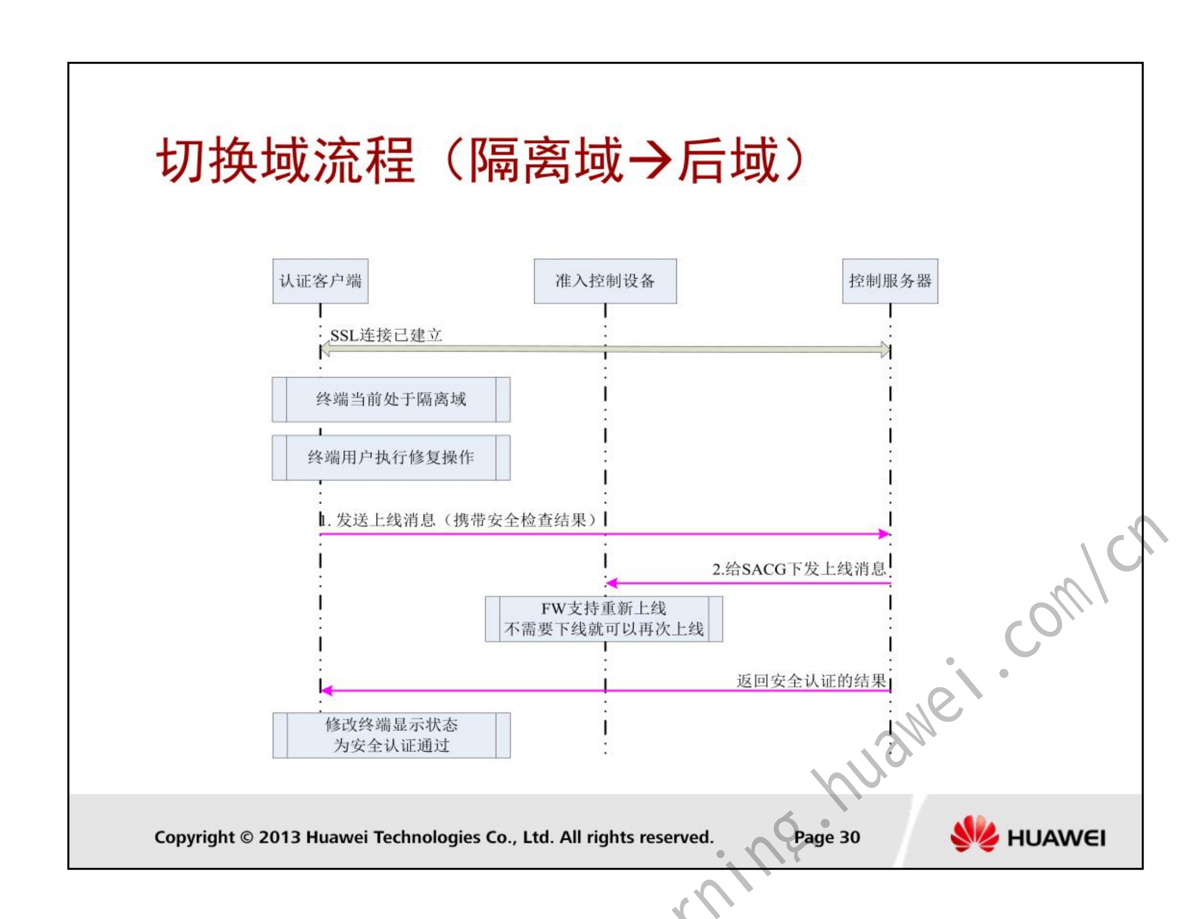
- 切换流程：终端被隔离后进行修复，修复完成后：
  1. 客户端发送认证消息
  2. Portal上线请求
  3. 用户已经在线
  4. 下发ACL
  5. 应答OK
  6. 终端上线OK



- 身份认证前，流量只能访问认证前域资源；安全认证后，在硬件SACG上动态生成ACL的防火墙规则。
- 对于无需安装客户端的机器：可以根据MAC、IP、MAC+IP不对其进行控制。



- SACG接入流程
    1. Agent与SC建立SSL连接
    2. 执行身份认证
    3. 请求安全策略参数
    4. Agent执行安全策略检查
    5. Agent把安全检查的结果上报SC
    6. SC根据安全检查的结果控制准入控制设备切换认证域
    7. SC返回安全认证结果，认证流程结束



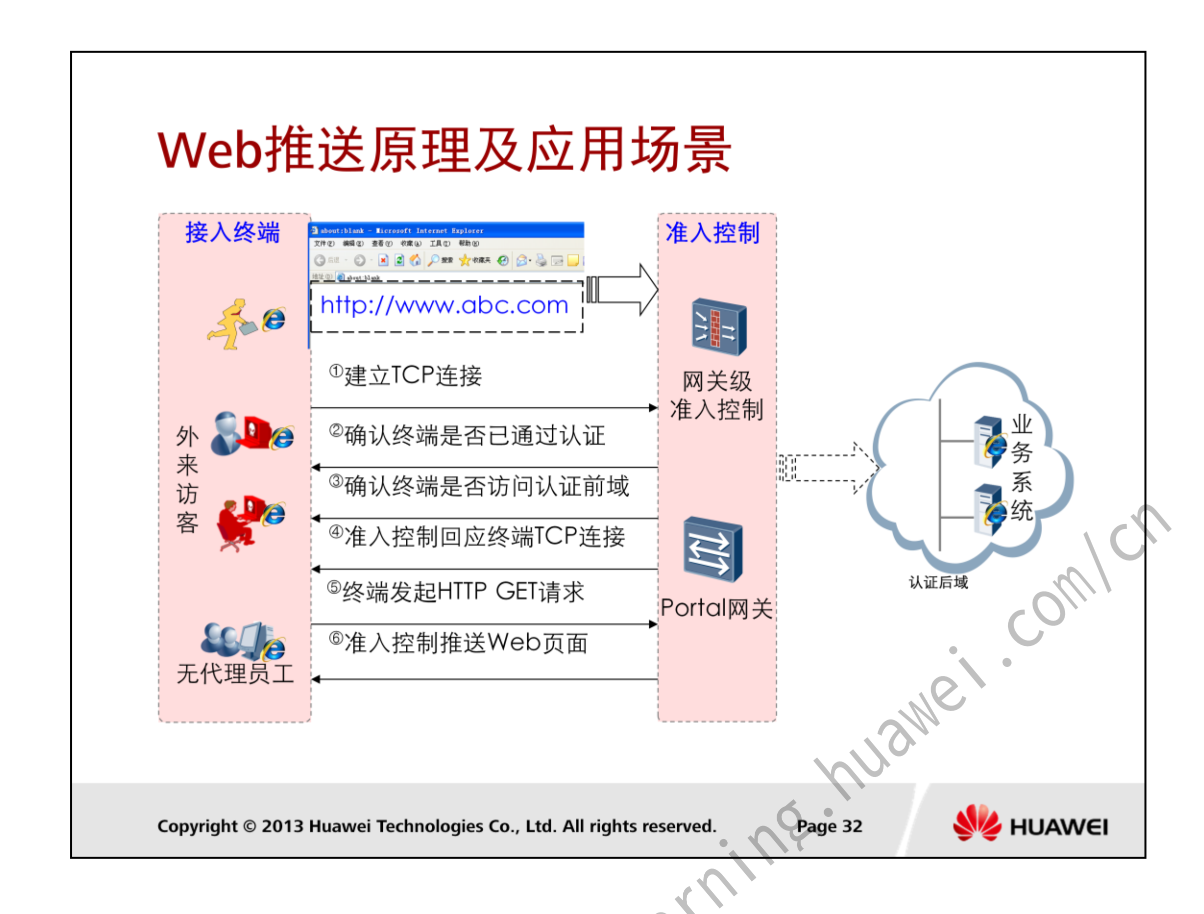
终端位于隔离域→终端用户点击修复(假设违规可以自动修复)→修复后自动进入后域

接入方案综合对比

	硬件SACG	软件SACG	802.1X	Portal	SACG+主机防火墙
适宜网络规模	任何规模网络	中小规模网络	小型网络	小规模网络	任何规模网络
部署和维护成本	低	中	高	中	中
管理控制力度	中	中	高	中	高
认证后域访问控制能力	高	中	低	中	高
可靠性	高	高	低	低	高

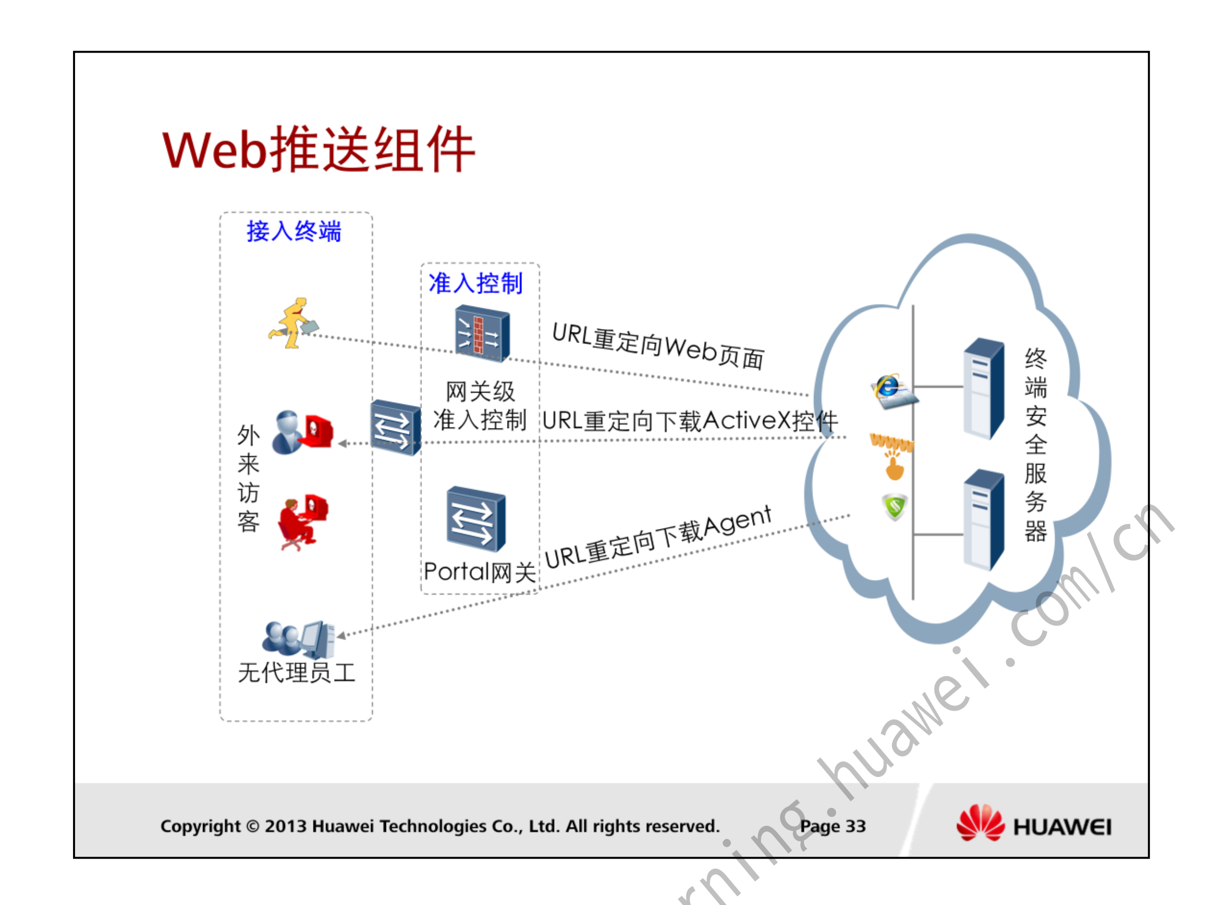


- 混合方案优势互补、效果最佳。
- 各种接入方案的不足：
  - SACG：终端间互访控制差：无法控制内部员工、访客、不合规终端间互访；
  - 主机防火墙：管理力度弱：无法强制安装客户端；
  - 802.1X：1）依赖二层设备支持802.1X；2）整体部署维护成本高；3）不同厂商或不同型号设备的802.1X特性存在较大差异，影响部署和客户体验。

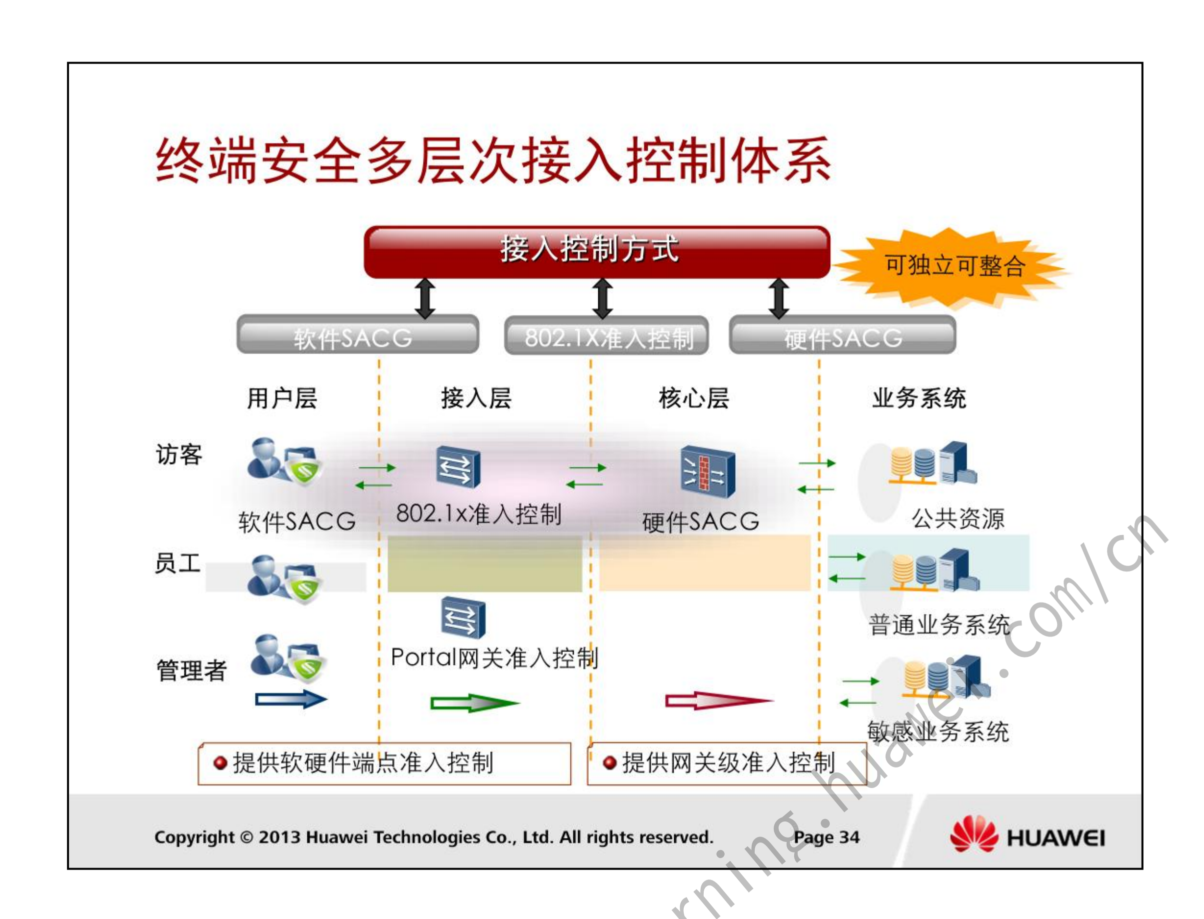


支持Web推送的准入控制设备，硬件SACG、Portal网关。

- 前提条件
  - 终端主机使用浏览器访问网络，流量经过准入控制设备；
  - 终端还没有通过身份认证，并且需要访问的资源不在认证前域；
  - 终端若通过域名访问，需确保域名可解析且DNS服务器部署在认证前域。若通过IP地址访问，需确保IP地址是合法的单播地址；
  - 终端访问非认证前域流量需可路由，以触发Web页面推送机制。
- 原理
  - 准入控制伪造目标计算机与终端建立TCP连接；
  - 准入控制设备通过HTTP重定向实现WEB推送功能。
- 特点
  - 终端任意访问一个IP地址（需IP地址在硬件SACG准入控制设备上路由)，都可以实现WEB推送，该IP地址不需要存在，只需要流量经过SACG；
  - 如果使用域名，要求该域名能够解析，如果域名不能解析，则终端无法发起TCP连接。



- 进行内网终端的准入条件是需进行身份认证，认证方式主要存在三种方式：Web、ActiveX(WebAgent)、Agent。
- Web只能提供身份认证，不能进行安全认证，适用于只需进行访问Internet的外来访客；
- Web Agent除了能进行身份认证外，还能进行部分安全认证，适用于访问企业内部非敏感业务资源的外来访客；
- Agent能提供强大的身份认证和安全认证，企业内部终端一般采用此方式。



Portal网关若与802.1X交换机进行准入控制整合时，需确保他们不是同一台交换机设备。



目录

1. 终端安全设计思想概述
2. **终端安全技术**
   - 2.1 终端安全技术概述
   - 2.2 身份认证
   - 2.3 接入控制
   - **2.4 安全认证**
   - 2.5 业务授权与审计
3. Policy center 系统简介
4. 终端安全系统设计



- 本节主要介绍实现终端安全所使用的技术。

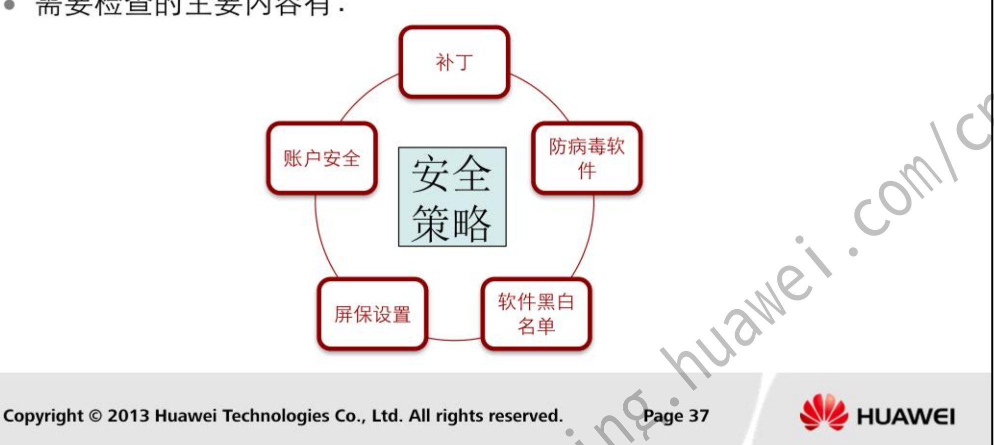
安全认证

- 安全认证是指系统对终端主机和用户行为进行监控和认证，如果认证不通过，则终端将会被禁止接入业务网络，主要包括以下几个方面：

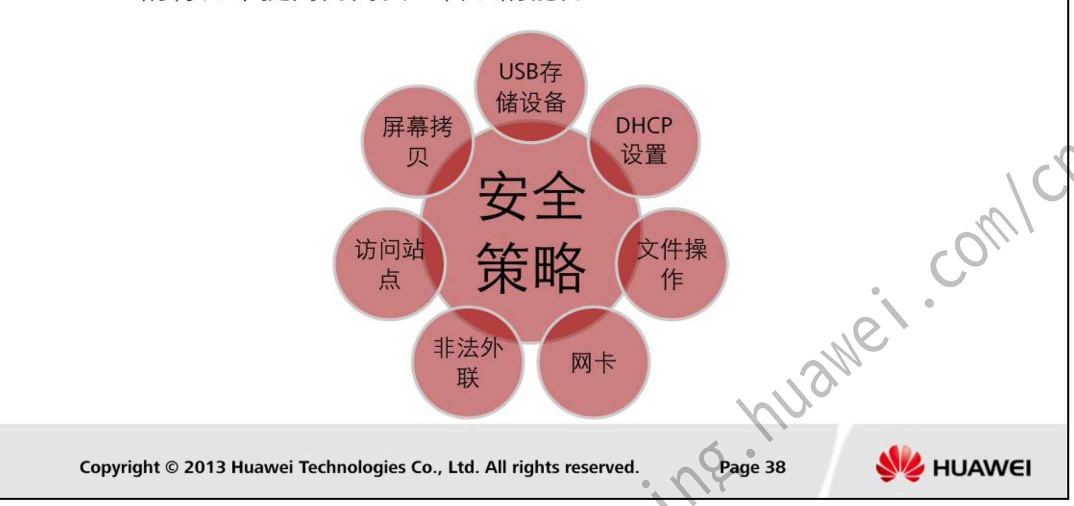
终端主机安全管理					终端用户行为安全管理					
补丁管理	账号管理	防病毒软件	屏保设置	软件黑白名单	USB存储设备	DHCP设置	文件操作	网卡管理	非法外连	访问站点



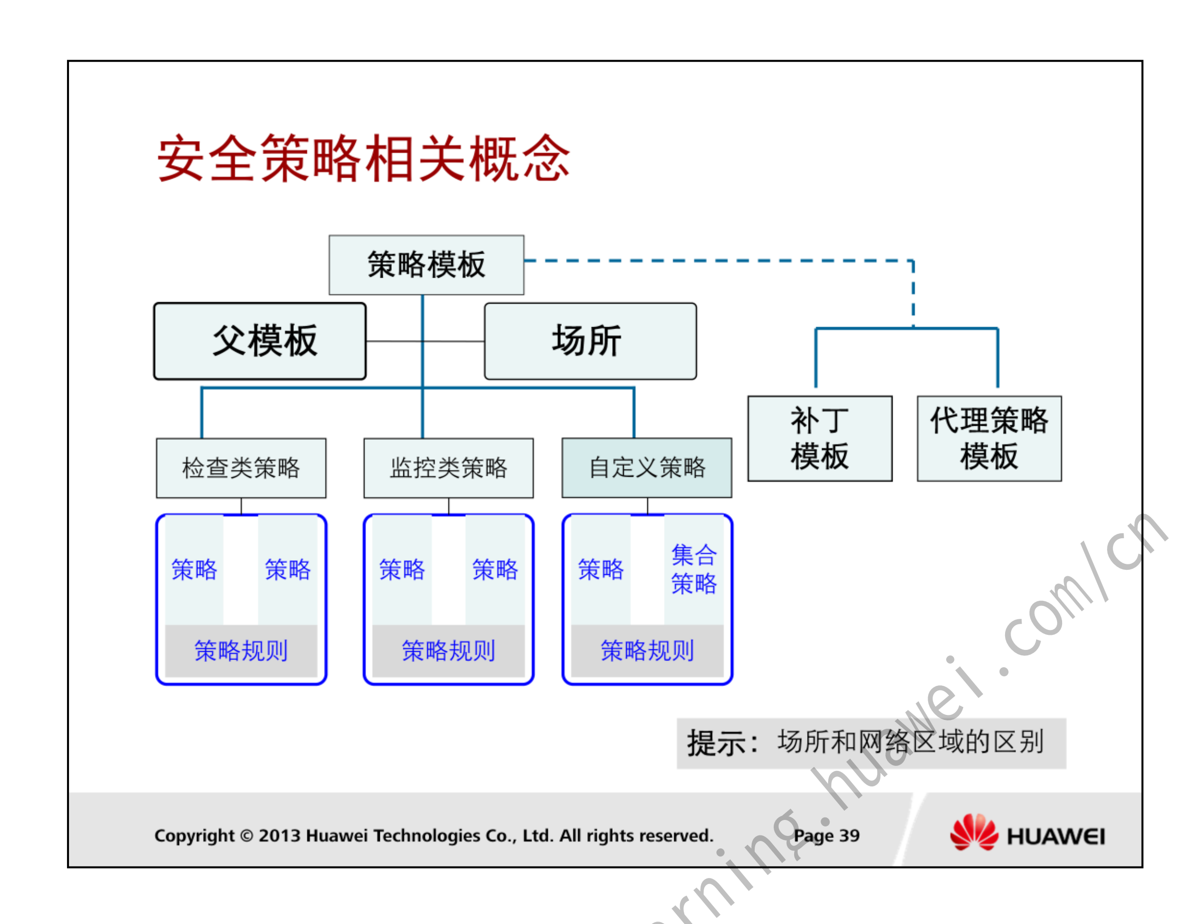
- 安全认证主要包括两个方面内容：
  - 检查终端安全情况：补丁、软件、屏保、防病毒软件等是否符合定制策略。
  - 监控用户行为：文件操作、USB的使用、网卡的使用、访问的站点等是否符合定制策略。



- 可以提供基于Microsoft Windows、Linux操作系统的终端主机的安全策略检查功能，对终端主机的系统配置状况、安装的软件信息、屏保配置、本地冗余账号等进行检查，并支持对操作系统补丁、Office补丁、IE补丁、SQL Server数据库补丁的更新情况进行检查并自动下载补丁，检查病毒库更新状态。
  - 补丁管理：检查终端主机已安装操作系统及相关软件补丁并记录未安装的补丁。在终端用户未安装指定的补丁时，终端代理和Web Agent插件提供自动和手动两种方式安装补丁。
  - 防病毒软件管理：检查终端主机是否安装指定的防病毒软件、防病毒软件的版本及病毒库的更新周期是否符合要求。
  - 软件黑白名单：在终端主机上检查已经安装的软件是否合法，或者需要强制安装的软件是否尚未安装。
  - 屏保设置：检查终端主机的屏幕保护参数设置是否满足安全策略的要求，包括是否启用屏幕保护功能、是否启用密码保护功能以及屏幕保护启动时间。
  - 账户安全：检查Microsoft Windows操作系统账户的密码是否身体符合要求。
  - 其他可检查的内容：共享文件、注册列表，共享打印机等。
- 终端代理支持在如下两个阶段执行安全策略：
  - 在代理启动后执行安全策略，如屏保设置是否符合规格、是否安装必须要安装的杀毒软件等。
  - 在终端用户通过身份认证后执行安全策略，资产管理、上网行为的管理等。



- 监控USB移动存储以管理员预设的USB存储设备的访问控制策略开放终端用户对USB存储设备的访问权限，并记录终端用户访问USB存储设备的日志。
- 监控终端主机是否采用DHCP（Dynamic Host Configuration Protocol）方式获取IP地址。
- 监控终端用户是否非法连入Internet。
- 监控屏幕拷贝策略能够确保机密电子文档（例如DWG图片、AI图片或DOC文档）不会被终端用户通过"PrintScreen"键截取屏幕非法保留或传播。
- 监控访问站点，通过配置网站的URL（Uniform Resource Locator）地址禁止终端用户访问某些网站，或允许终端用户访问某些网站。
- 监控终端主机的网卡连接状态和无线网卡，并提供禁用无线网卡功能。
- 监视终端用户在终端主机的本地硬盘（不包括映射网络驱动器中的文件和远程共享的文件）进行的文件操作。



策略模板是若干策略的集合。为了审计不同终端主机的安全状况和终端用户的行为，管理员需要定制不同的策略模板用于保护和管理终端主机。当终端用户进行身份认证和安全检查时，终端代理执行与终端用户相关联的策略模板中的所有策略。

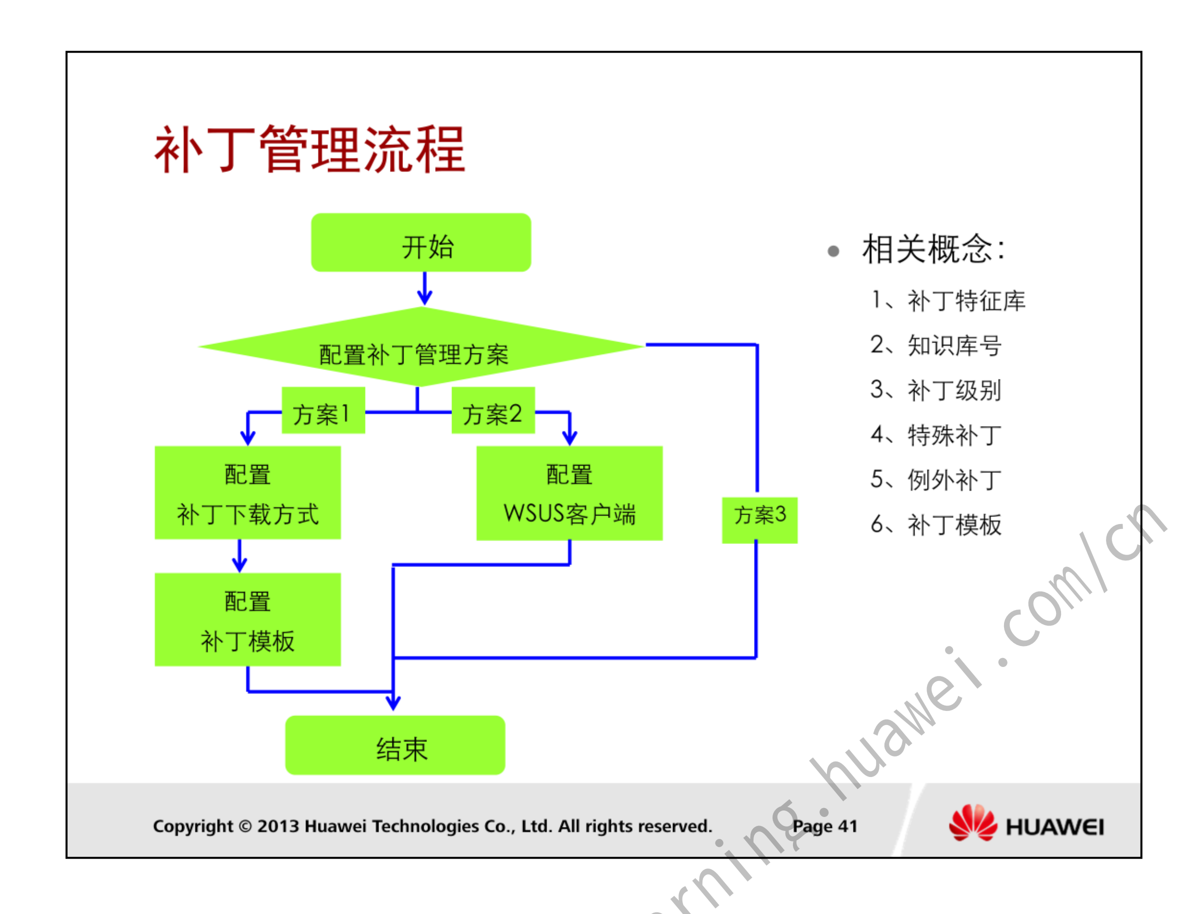
策略模板与父策略模板是相对的，可以把公司的策略定义为父模板，部门在继承公司策略的基础上，编辑部门的策略。策略模板在引用或继承父策略模板时只能以策略为单位，不能以策略规则为单位进行继承。策略模板主要分检查类策略、监控类策略和自定义策略。而补丁模板和代理策略模板是独立于策略模板外的另一种模板，补丁模板关注的是给指定组织下发和安装补丁，一般情况下需与策略模板中的补丁策略进行联动实现；而代理策略模板是提供给终端代理进行局部参数配置的模板，如授权给某些组织终端强制终端防卸载、禁止终端保存密码、终端密码策略、远程协助和禁止终端修改密码等策略。

场所是指终端用户使用某种方式接入受控网络办公时的终端环境。随着IT信息化在企业的重要性越来越高，终端用户的办公场所越来越多样化，有些员工在公司内办公，有些员工在家里办公，而有些员工长期出差，办公地点不确定。同时，终端用户接入网络的方式也各有不同，例如：通过局域网、无线网络、VPN等方式接入。在进行策略管理时，如果不考虑终端用户的场所，将可能导致在不同场所下终端用户不能正常接入受控网络办公。基于这种原因，引入了场所概念以适应不同应用环境，终端代理默认只支持缺省场所。缺省场所是指没有定义使用场合的场所，表示不区分终端用户的使用场合。当按场所进行策略管理业务时，请根据业务需求联系厂商定制场所文件。



补丁管理功能，帮助终端用户解决系统漏洞修复工作，提高企业终端主机的安全水平，降低IT（Information Technology）系统维护成本。

- 补丁管理的主要功能如下：
  - Microsoft Windows操作系统补丁、Microsoft SQL Server数据库补丁、Microsoft Internet Explorer补丁、Microsoft Office补丁，以及Linux补丁。
  - 自动下载补丁。 TSM管理器能够自动从微软网站下载补丁（允许服务器通过代理连接互联网），支持从上级管理器同步补丁。
  - 提供补丁信息列表。 给出从微软同步的补丁信息列表，包括补丁名称、补丁严重程度、补丁是否部署、补丁发布时间。对于某些补丁提供补丁的漏洞描述等信息。
  - 补丁部署情况列表。 对于要求部署的每一个补丁，查看补丁的部署情况，包括发现未部署该补丁的终端主机数和已经部署了该补丁的终端主机数。对于未部署该补丁的终端主机，查看终端主机列表，便于管理员查找未部署补丁的终端主机和实施管理。
  - 提供补丁下载历史记录。 提供补丁下载的历史记录，便于管理员查看以往的补丁下载情况。
  - 分布式补丁分发。 允许配置多台FTP服务器，设置其中一台为主FTP服务器，其他的为镜像FTP服务器。多台FTP服务器之间自动实现同步，允许管理员配置同步周期。



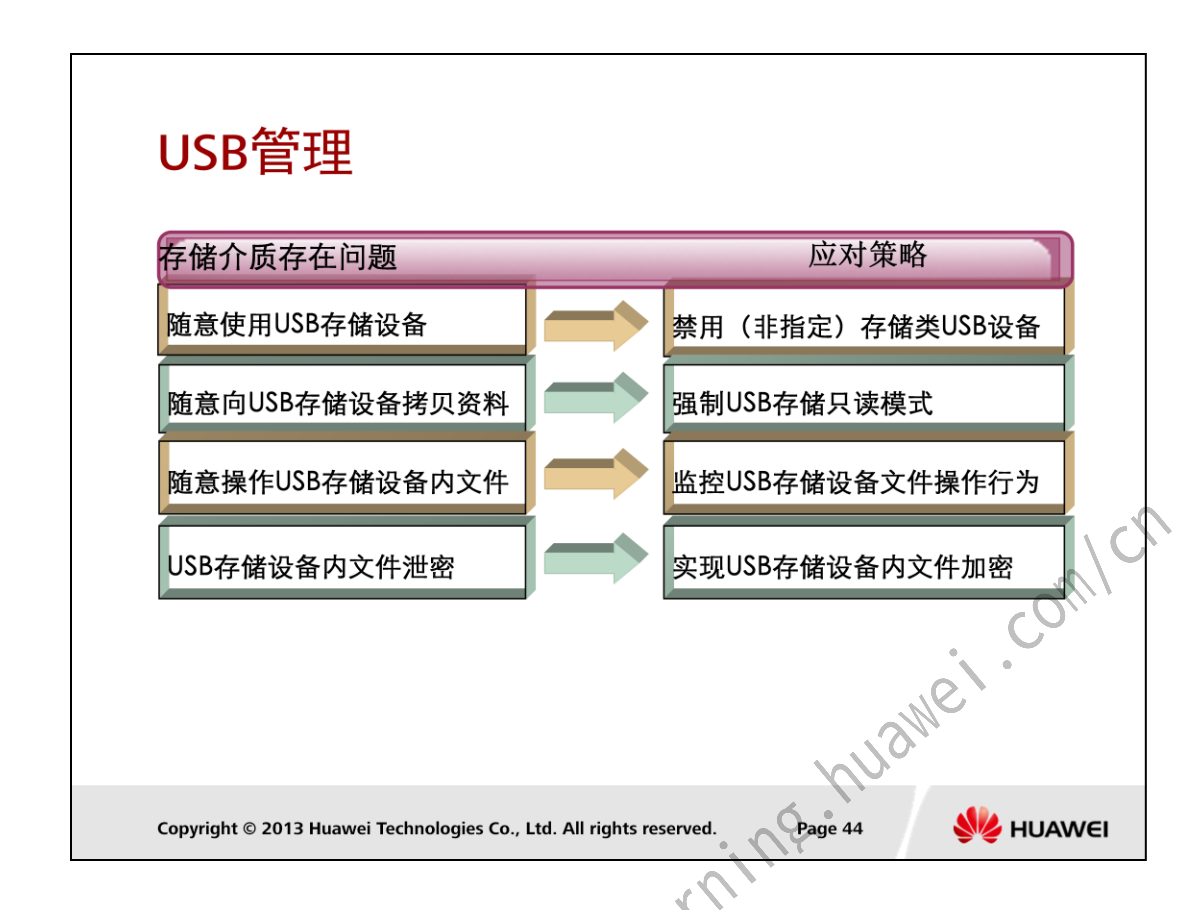
有三种Microsoft Windows补丁管理方式：1）使用系统自有的补丁下载和分发功能，与操作系统补丁检查策略联动完成补丁检查；2）使用微软WSUS系统的补丁下载和分发功能，与操作系统补丁检查策略联动完成补丁检查；3）不提供补丁下载和分发功能，操作系统补丁检查策略独立完成补丁检查。

Microsoft Windows补丁管理与Microsoft Windows补丁检查策略之间既有联系又有区别，他们均能检查终端主机是否已经安装指定的Microsoft Windows操作系统补丁，不同点在于：Microsoft Windows补丁检查策略重在检查终端主机是否安装Microsoft Windows操作系统的补丁，并且能够与检查结果对终端主机进行接入控制。当终端主机未安装指定的Microsoft Windows操作系统补丁时禁止终端主机接入受控网络，而不是协助终端用户自动安装Microsoft Windows补丁。在这种情况下，管理员必须配置Microsoft Windows补丁检查策略与Microsoft Windows补丁管理联动，或者与WSUS联动才能实现自动安装Microsoft Windows补丁，否则，终端用户只能手工下载并安装补丁才能消除违规。

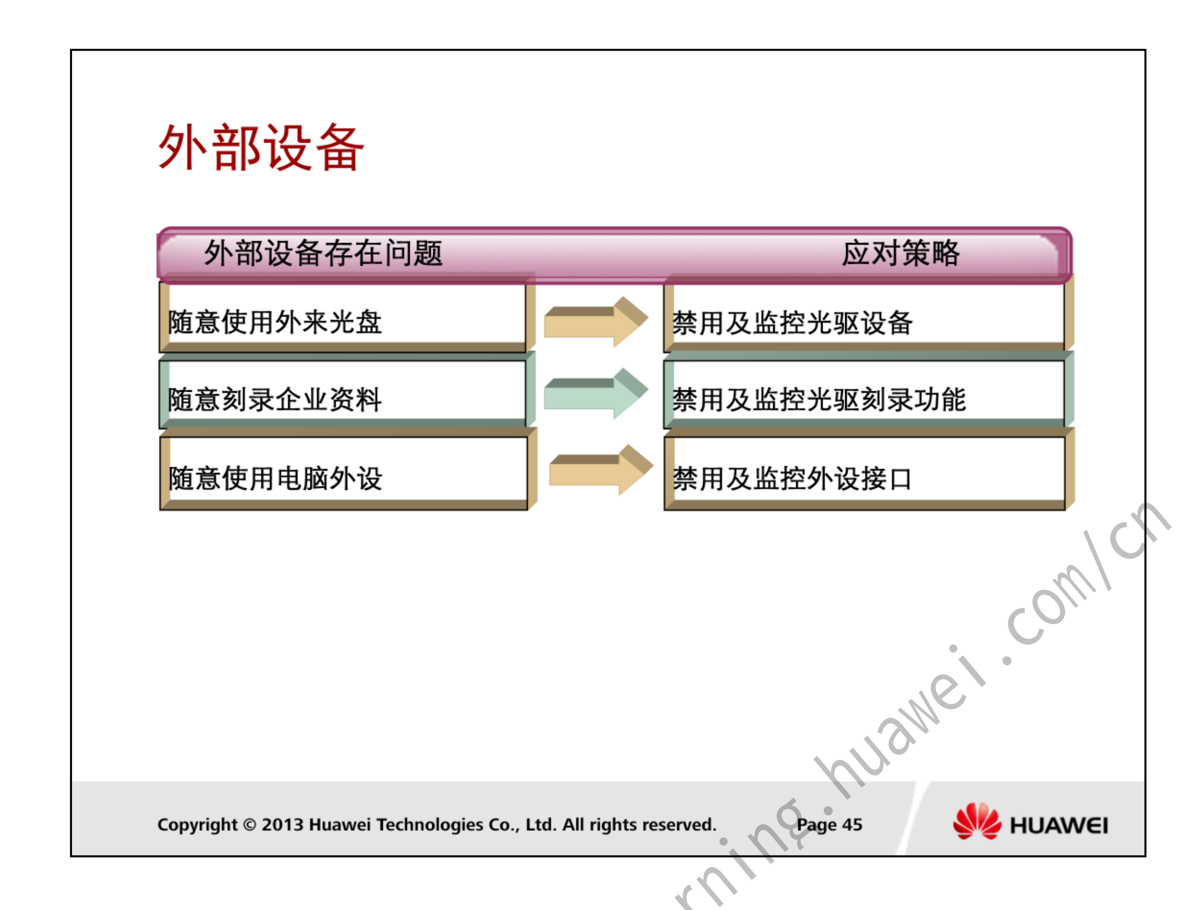
相关概念：1）补丁特征库，是指包含Microsoft Windows操作系统补丁相关信息的文件，方便终端安全系统获取各个补丁在微软网站下载的URL地址，并且提取补丁的详细信息。补丁特征库一般为“wsusscn2.cab”文件；2）知识库号，是指微软为解决Microsoft Windows操作系统发现的问题而发布的文章的编号，一个知识库号可代表一个操作系统补丁；3）补丁级别，是指该补丁修正的缺陷对Microsoft Windows操作系统自身形成安全威胁的影响程度；4）特殊补丁，是指在终端安全系统从微软官方网站下载Microsoft Windows补丁时，需要优先下载的补丁；5）例外补丁，是指不需要终端代理或Web Agent插件在终端主机检查是否已经安装的Microsoft Windows操作系统



- 企业信息安全面临的挑战：
  - 无法控制外来移动存储设备的随意接入。外来移动存储设备随意通过终端主机接入企业网络，带走机密数据，而且移动存储设备携带的病毒容易感染终端主机。
  - 无法保证内部移动存储设备丢失后导致的信息外泄。移动存储设备未进行任何安全保护，企业保存重要信息的存储设备外出丢失后导致重要信息外泄。因无法对存储设备使用进行授权控制，企业普通存储设备内部丢失后无法保证不被随意访问而导致信息外泄。
  - 无法保证数据的安全交换。移动存储设备不做任何控制，无法解决移动存储设备在内外网间、安全等级不同的网络交换时容易导致数据外泄的问题。
  - 病毒快速蔓延。未进行移动存储设备免疫处理，容易导致U盘病毒在企业网中传播。



- 支持只禁用USB存储设备，既允许使用USB鼠标/键盘之类的非存储设备，而对于U盘/USB硬盘/USB光驱之类的存储设备完全禁用。或只禁用未注册USG存储设备；
- 支持USB设备只读控制，既允许使用USB非存储设备，以及USB存储设备，对于USB存储设备，只允许读操作，禁止写操作；
- 提供USB设备文件操作的监控能力，能够识别并且记录文件操作。



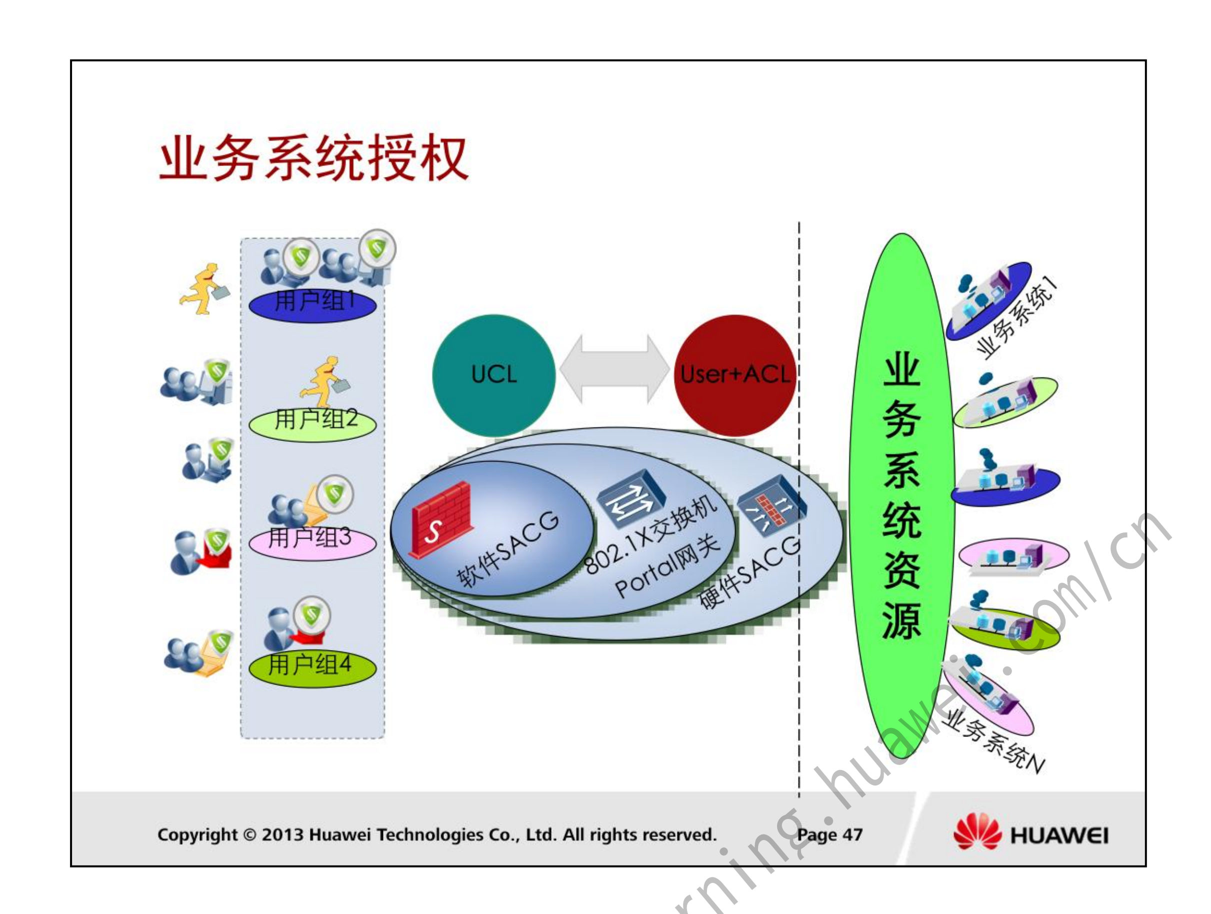
- 监控光驱策略，不既可以监控普通光驱设备的使用，还可以监控刻录光驱的使用；
- 系统设备（如打印机、蓝牙、红外、SD/MMC控制器等），通过监控这些系统外设可防止信息资产泄露的可能。



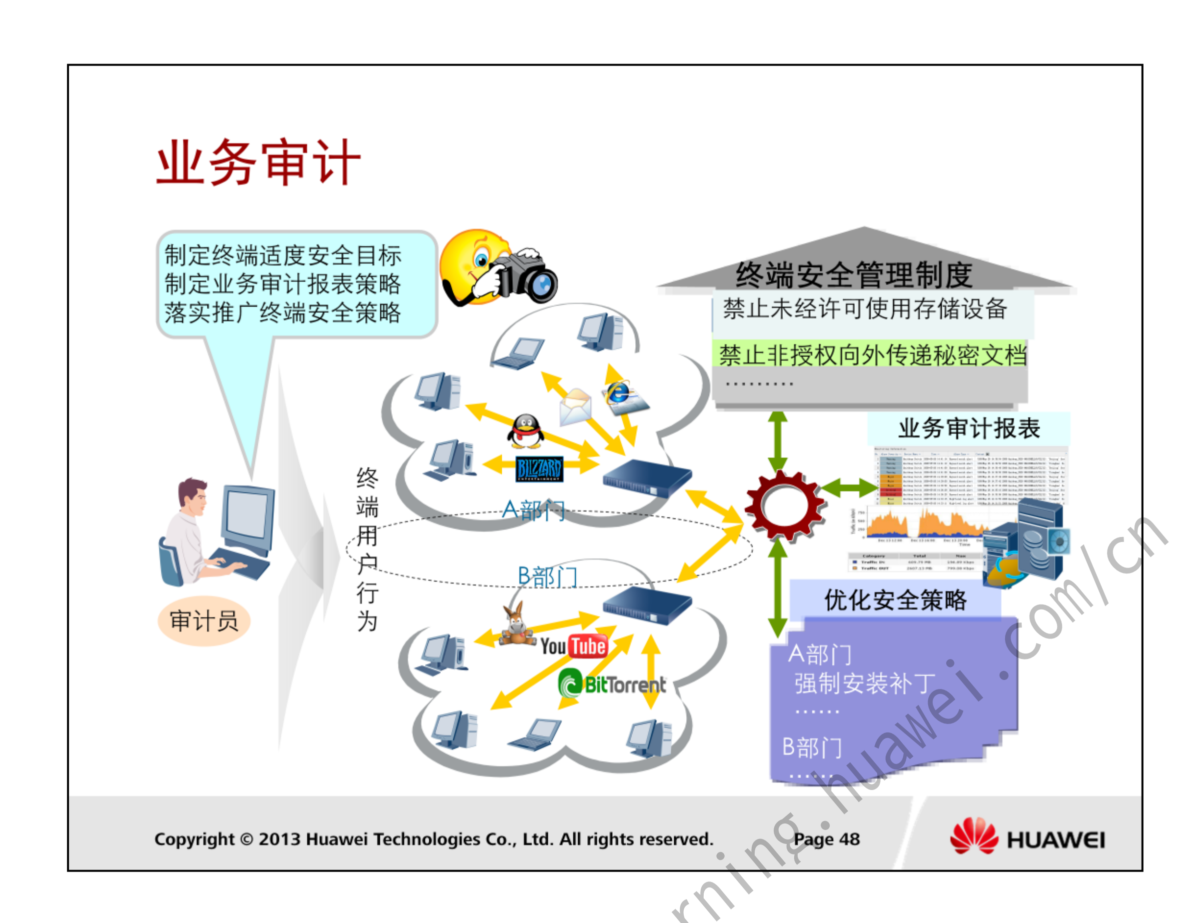
目录



- 本节主要介绍实现终端安全所使用的技术。



业务系统资源的业务授权目前主要支持软件SACG、802.1X交换机、Portal网关和硬件SACG，其中采用的实现机制是基于User的ACL,既UCL。终端用户只能通过身份认证和安全认证后，将会获取系统授予的访问权限策略（UCL）。



通过输出各种日志信息以及报表信息对业务进行审计。



目录



本节主要介绍华为终端安全系统Policy Center。

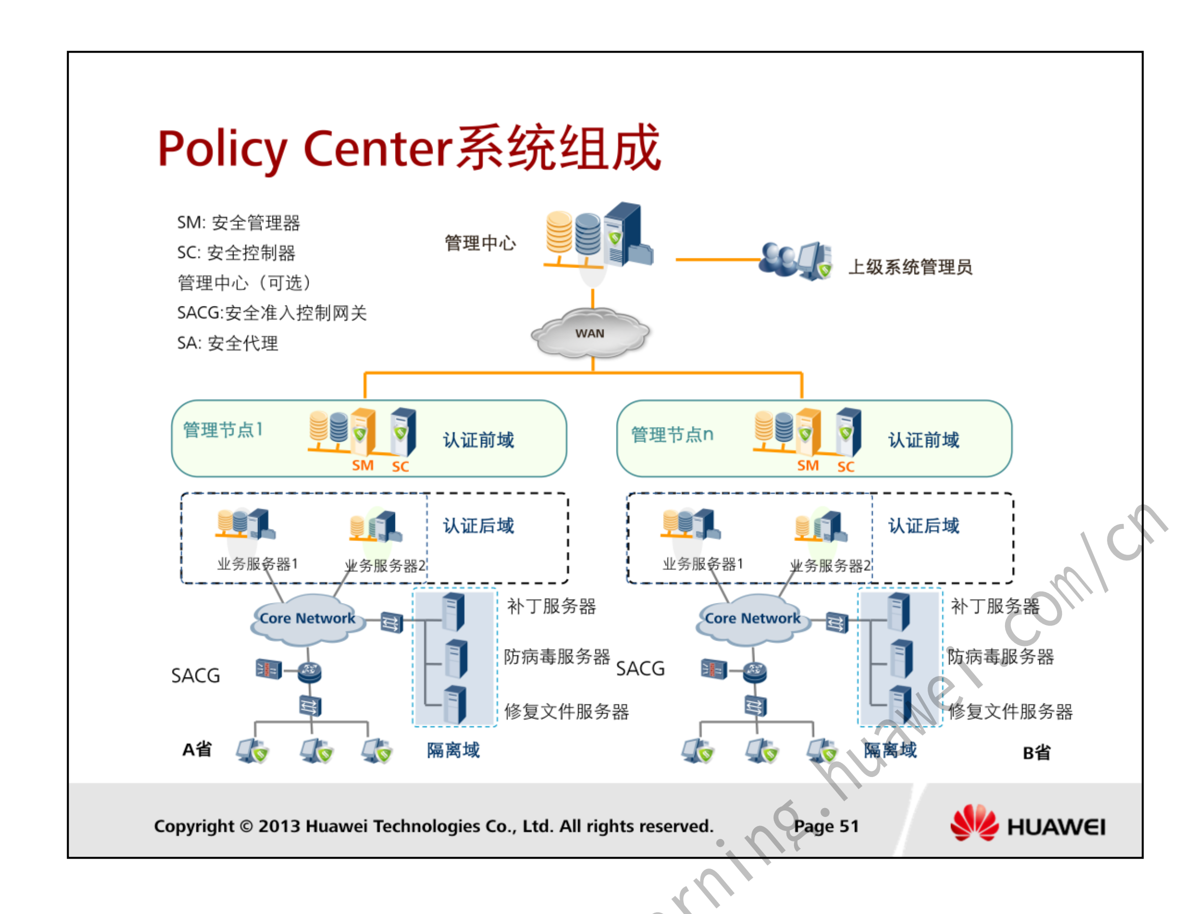
Policy center 简介

- 为了解决企业内部网络管理失控的问题，保障企业内部网络的畅通、终端主机的安全和公司信息数据的安全，实现企业网络安全建设的目标，华为公司推出了新一代终端安全产品Policy center。



华为策略管理中心Policy Center 提供统一的策略引擎，在整个组织内实施统一访问策略（有线、无线，内网，外网一体化），实现基于用户、设备类型、资产类型、接入时间、接入地点、接入方式的认证和授权，满足企业接入认证多层次、泛终端接入的需求;同时提供全生命流程的访客管理，给访客提供一个随时随地上网的空间，提高访客工作效率，提升企业品牌形象，降低IT 运维的压力；丰富的安全策略，提升终端安全等级，阻止不安全的终端以及不满足企业安全策略的终端接入网络提升终端的安全性，符合企业的管控策略，提升整体的信息安全水平。

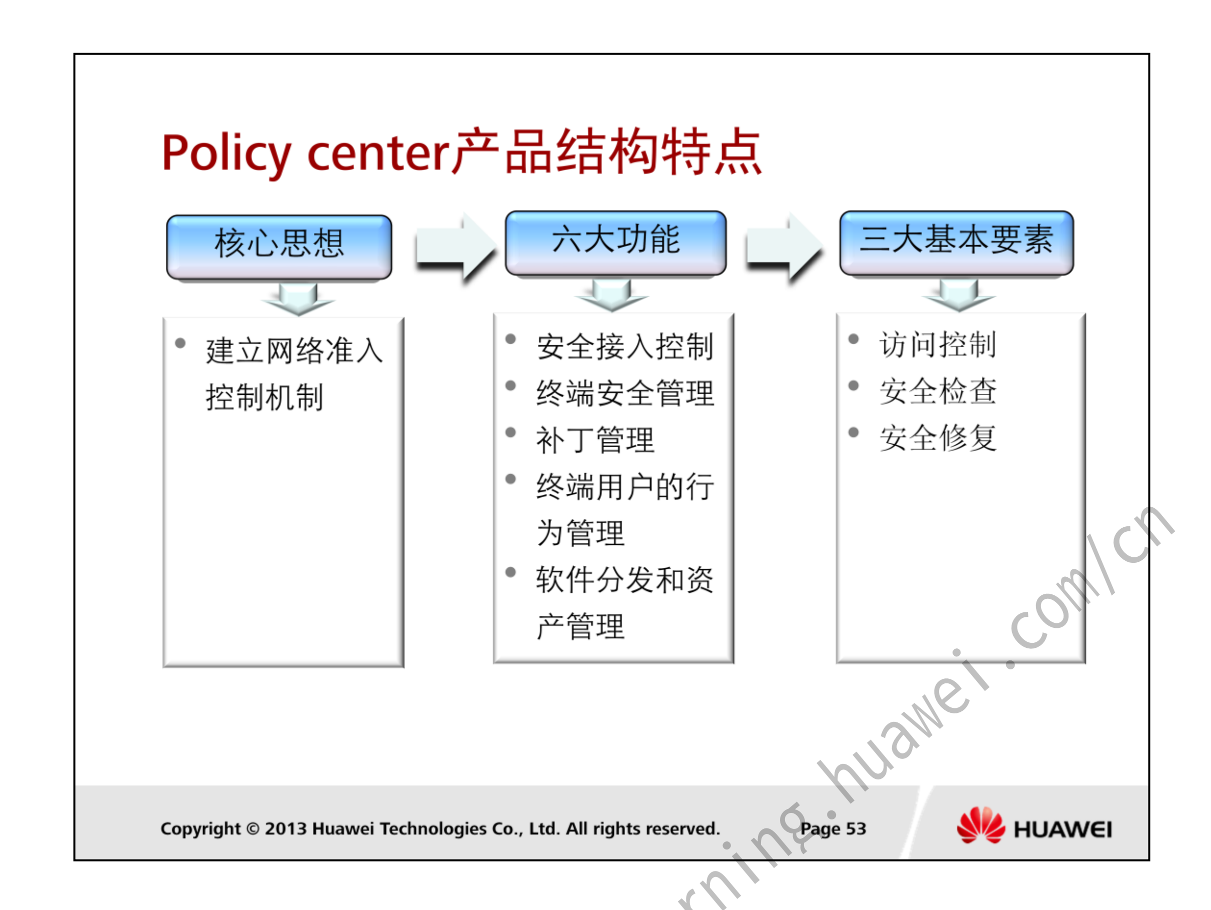
Policy Center系统初始账号：admin 密码：Admin@123



接下来我们来看一下Policy Center终端安全管理的系统组成,SM和SC构成Policy Center服务器部分。

- 管理中心：适用于分级部署组网方案，安装在总部，主要提供分级管理功能，接管位于下级的安全管理器节点。
- SM：作为系统的核心管理服务器，管理多个SC；SM采用B/S架构，系统管理员可通过Web界面配置和修改用户信息、访问权限和策略等，并完成报表输出
- SC：作为与SA交互的控制点，是系统管理功能的实施者。完成用户身份认证、安全策略下发和软件下发等任务。并与802.1X或SACG联动在完成身份认证和安全策略检查后，开放端口或匹配ACL规则授权用户访问网络资源。
- SA：安装于客户的PC机上，向服务器获取安全策略参数，根据这些参数执行本地计算机的安全策略检查；实施监控终端的行为，并且把审计的结果上报服务器，作为审计的证据。
- SACG：是公司电信级防火墙硬件平台上开发的专用的准入控制网关，是实现硬件网关准入控制方式的核心设备

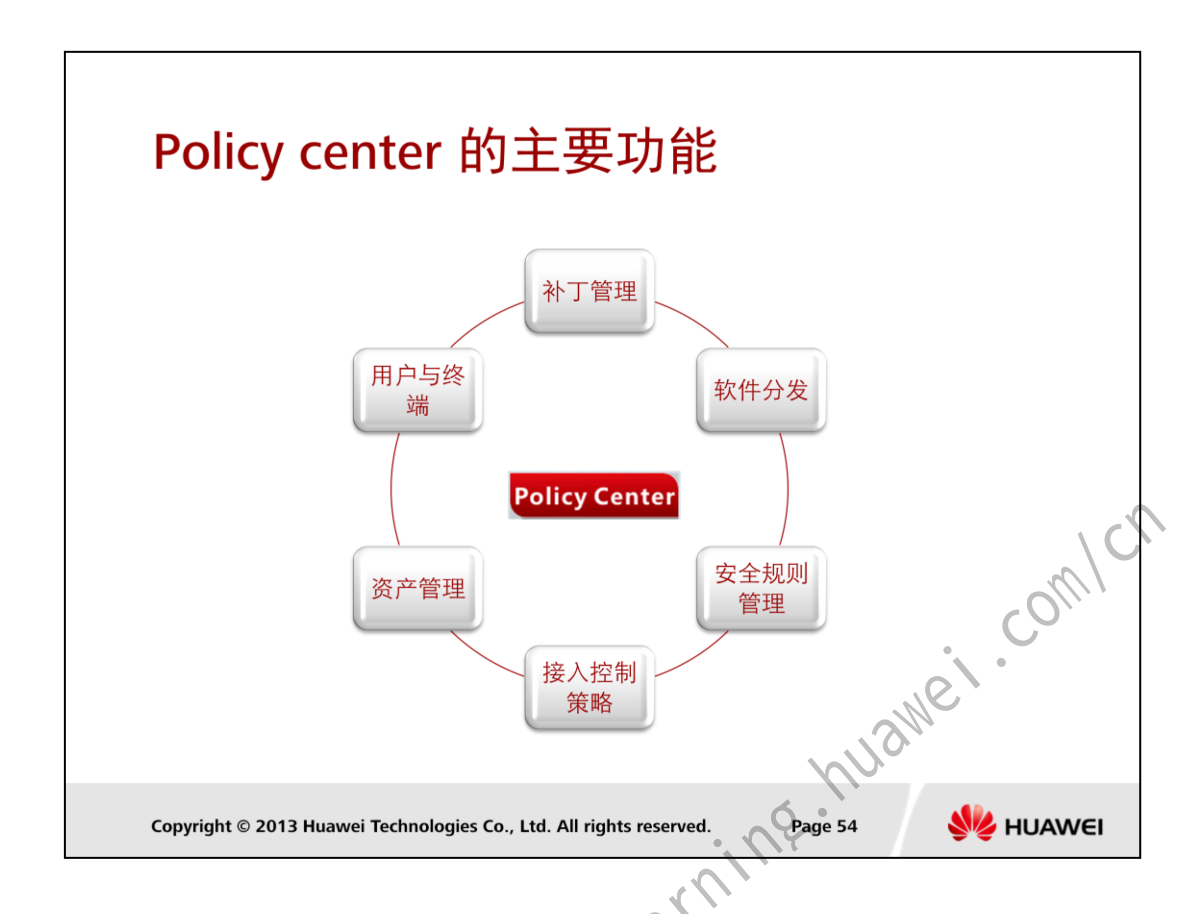
右图中显示了安全准入控制网关SACG方式的拓扑结构。据专业的网络安全评估专家建议，对网络内部终端和公共可访问的服务器到Internet或其他不可信网络的外出流量都应该进行过滤，以阻止黑客和蠕虫的“抓钩”攻击。SACG对终端的所有上行流量进行过滤，将网络分为......可信、非受信和DMZ(Untrusted,trusted和DMZ)三个域，用户在没有通过身份认证和安全检察前只能访问DMZ即受限的认证前域，通过后才能基于用户角色开放相应可以访问的认证后域，提供有效的内网接入保护。



Policy center基于代理为企业提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发和资产管理六大功能。其核心思想是建立网络准入控制机制，基本要素是安全检查、访问控制和安全修复。有效控制网络日渐增多的接入点，包括企业员工、外部访客、合作伙伴和临时雇员等对网络的访问，发现并隔离带有威胁的终端主机，提升网络防御安全威胁的能力。

Policy Center与网络接入控制设备配合，可以为企业网络提供网络接入控制功能和访客管理功能。Policy Center支持多种类型的网络接入控制设备，包括WLAN的AC/AP设备、华为的Portal交换机、通用的标准802.1X交换机，以及华为的SACG网络接入控制网关等。

Policy Center支持多种类型的接入设备，包括Windows PC、Linux PC、Andriod和Iphone/ipad等设备。其中对于Windows PC和Linux PC，如果这些设备部署和NAC客户端，可以在网络准入控制的基础上，提供更多的功能，包括终端的合规性检查、移动存储介质管理以及补丁管理、软件分发等。



- Policy center的主要功能特性包括：
  - 接入控制策略：支持普通账号、MAC地址和移动证书等身份认证方式，实现对企业员工、外部访客、合作伙伴和临时雇员等对网络访问的控制，保护业务系统安全。
  - 安全规则管理，全面评估终端主机的安全状态，强制隔离不安全终端主机，确保IT策略遵从，降低风险。终端安全状态检查主要包括检查是否安装各种补丁，是否安装企业要求必须安装或禁止安装的软件，终端主机安装的防病毒软件是否符合要求，是否启用ARP防护功能等。在检查结果的基础上，提供个性化的修复建议，协助安装各类补丁和必备的软件。丰富而全面的安全策略，提供基于部门和用户角色灵活的安全策略控制，强制终端主机遵循管理员统一制定的安全策略，协助管理员评估终端主机的安全状态，消除终端存在的安全隐患，以便主动降低终端主机的安全威胁，保障终端用户合理使用网络资源。
  - 补丁管理。 支持与WSUS（Windows Server Update Services）无缝集成，强制、及时、安全和准确的侦测系统漏洞，帮助终端主机及时更新补丁，避免由系统漏洞带来的安全威胁，可以对linux操作系统补丁进行管理如Ubuntu 9/10/11/12 、Canaima 3 、Debian 6操作系统。
  - 资产管理。 收集终端资产信息，跟踪资产变更状况，上报资产变更报表，资产变更后告警，且能够产生资产报表。
  - 支持将软件手工或按计划分发到终端主机，并支持按部门、按操作系统、按IP地址段进行分发。

Policy center系统部署介绍

终端数及可靠性要求	部署方案	硬件服务器数量
1～2000，无备份	硬件服务器1：管理器+控制器+配置数据库+日志数据库	1台硬件服务器
2000～10000，带控制器备份	硬件服务器1：管理器+控制器+日志数据库 硬件服务器2：控制器+配置数据库	2台硬件服务器
1～10000，带控制器、数据库备份	硬件服务器1：管理器+配置数据库 硬件服务器2：控制器+镜像配置数据库+备份日志数据库 硬件服务器3：控制器+见证服务数据库+日志数据库	3台硬件服务器
10000～20000，带控制器、数据库备份	硬件服务器1：管理器+日志数据库+见证服务数据库 硬件服务器2：控制器 硬件服务器3：控制器+配置数据库+备份日志数据库 硬件服务器4：控制器+镜像配置数据库	4台硬件服务器

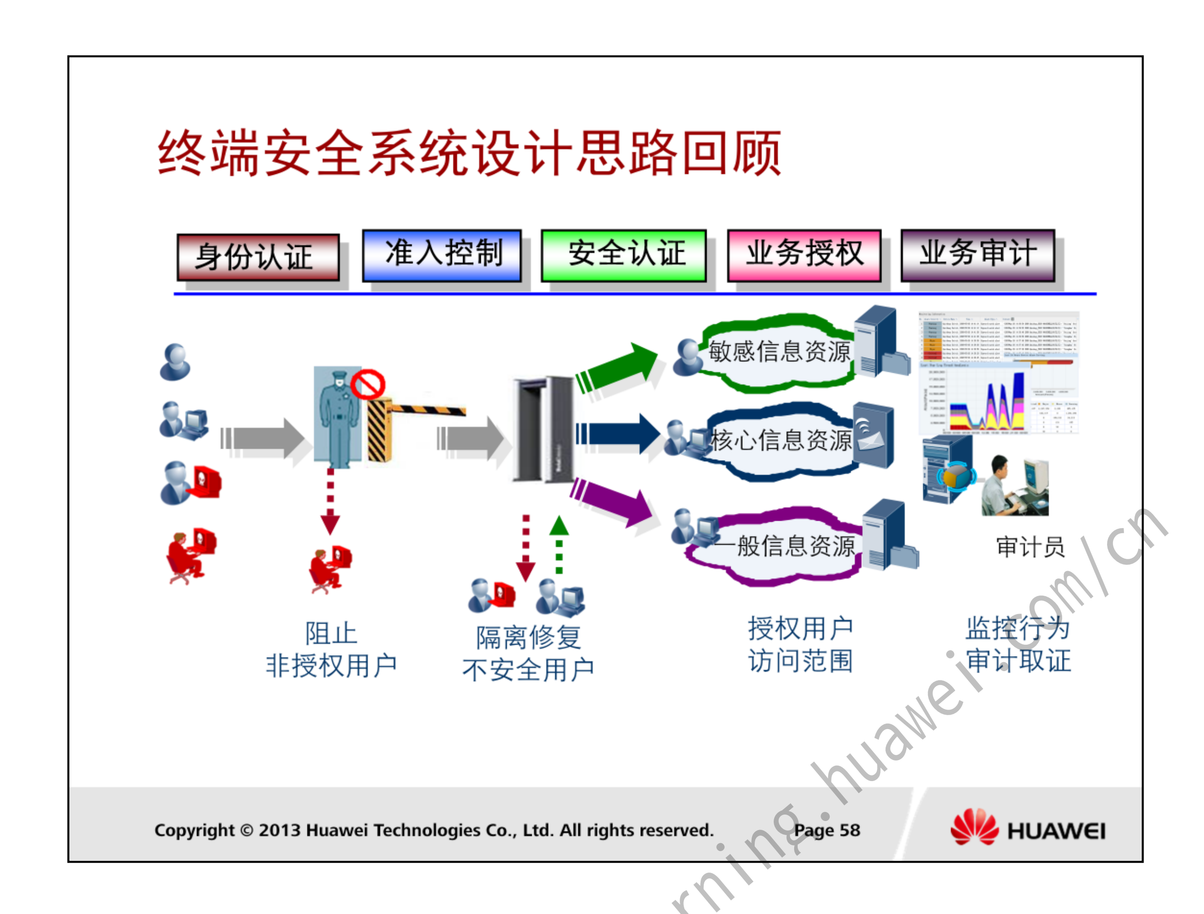


有关数据备份的知识点，在系统可靠性章节进行详细介绍。



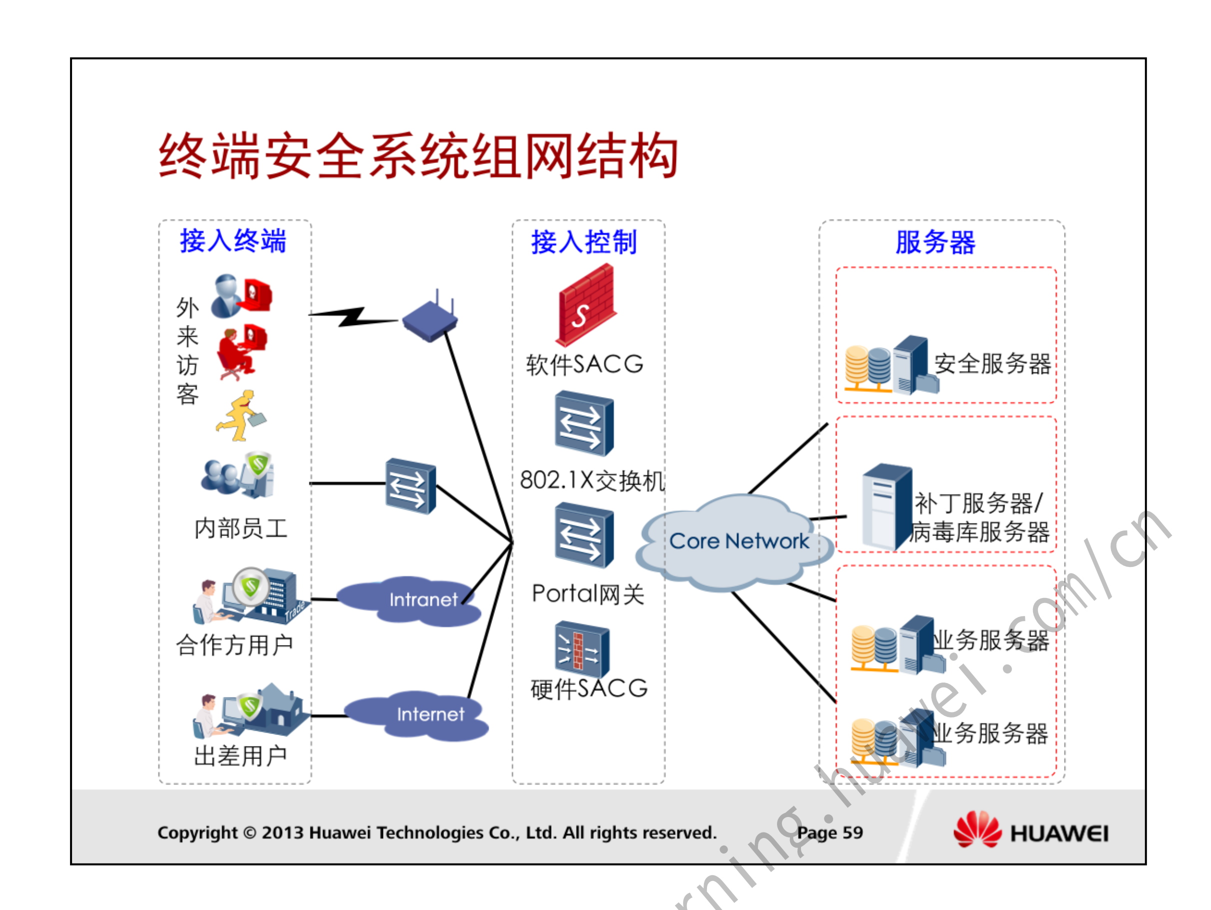
目录





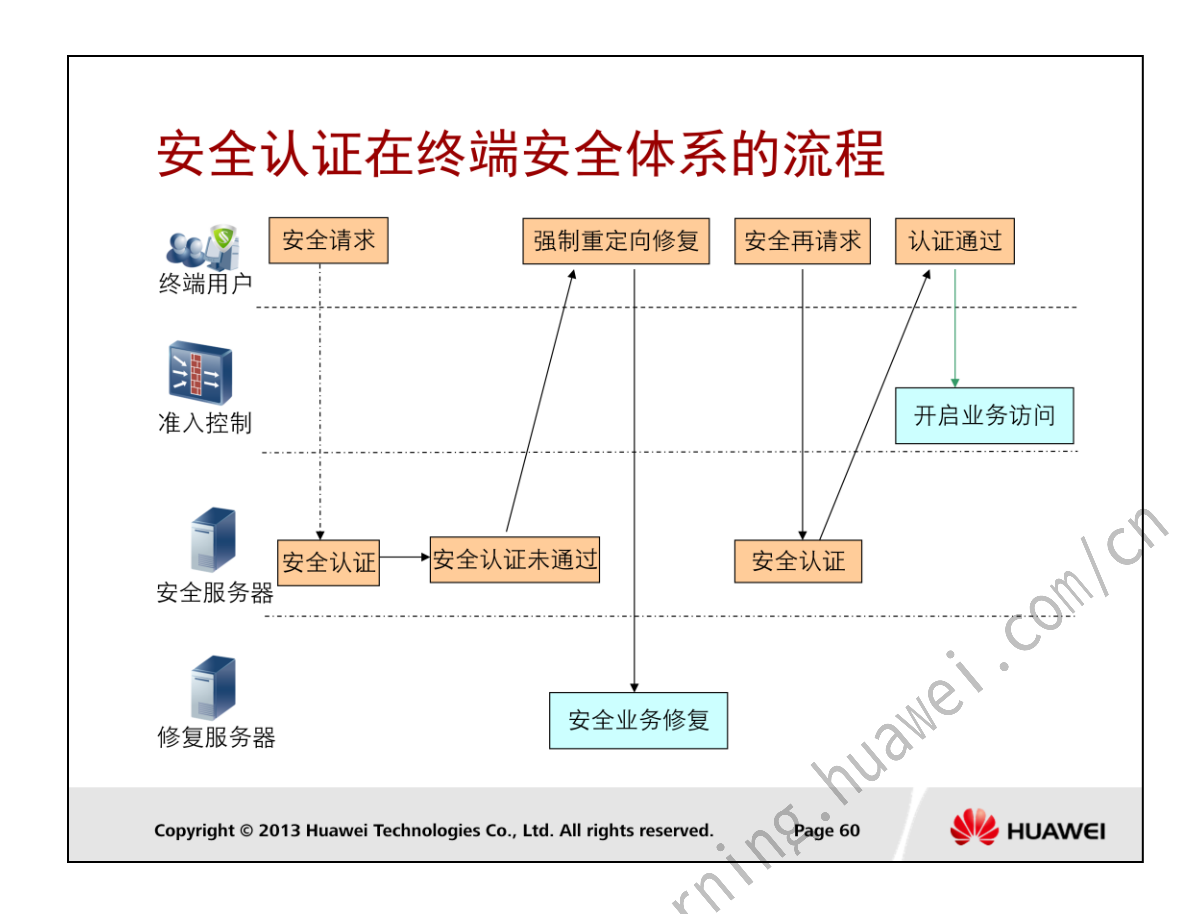
一体化防御体系主要由 5 大要素组成，即身份认证、准入控制、安全认证、业务授权、业务审计。其中身份认证是一体化防御体系的基础，准入控制是保障，安全认证和业务授权是手段，而业务审计是实现一体化防御体系的PDCA前提条件。各个要素在一体化防御体系中各持其职、分工合作，形成一个整体以构建完整的终端安全体系架构。

备注：信息资源即包括应用服务资源，也包括信息文档资源；



准入控制技术最主要的作用是把非授权终端用户阻挡在企业网络之外，而把授权终端用户（通过身份认证和安全认证的绿色终端）放进来。

- 软件SACG/终端互访控制：是内置在终端Agent上的一个组件；
- 标准802.1X交换机：支持业界流行802.1X交换机，如华为、H3C、CISCO；
- PORTAL网关：华为交换机的3300\5300系列交换机（软件版本V100R006），能够作为PORTAL网关，实施准入控制；
- 硬件SACG：系统可以与全系列华为中低端防火墙联动（如USG系统）。

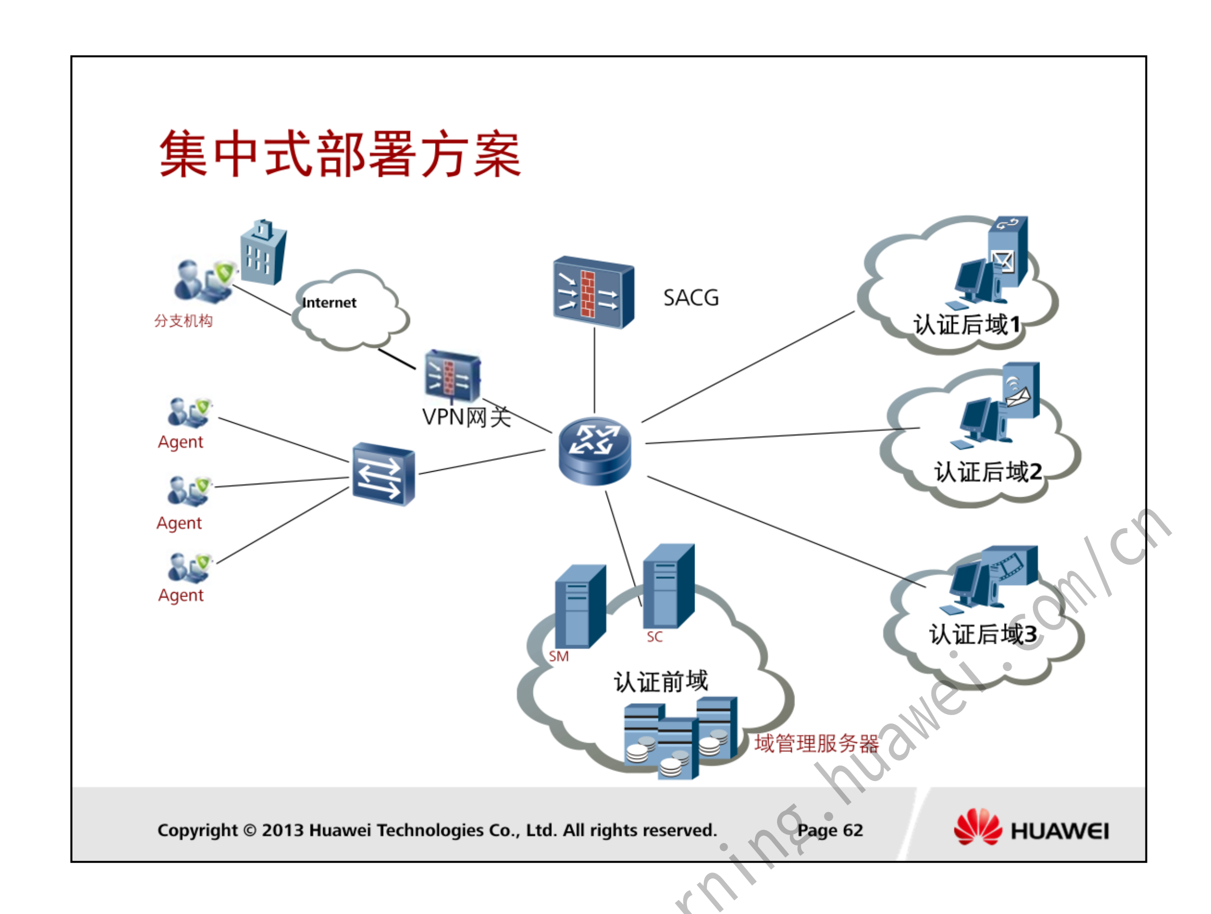


- SACG接入认证的原理和流程：
  - 用户终端接入企业标准网络时,SA代理会与SC控制服务器建立一个SSL通道，用于保护代理SA和服务器之间的通信；
  - 接下来,SA与服务器协商认证的参数以及License控制信息；
  - Liscense验证后,执行身份认证流程：SA根据采用的身份认证类型（用户名+口令/AD域集成认证等），将用户名/口令信息上报至服务器进行身份认证；如果是域认证方式(如AD\ED和第三方LADP系统等)，将与域管理服务器联动,使用域系统作为统一第三方认证源,用户无须再次输入用户名/口令即可认证；
  - 身份完认证成功后，SA向服务器请求更新安全策略，获得最新的策略信息列表，根据策略执行本地安全策略检查,最后将结果上报SC；
  - SC收到安全认证的结果，判断是否符合策略规定的接入要求，如果满足，则与SACG联动，通过用户的身份属性匹配ACL规则,把对应的终端从认证前域切换到认证后域，实现最小授权访问的目的；



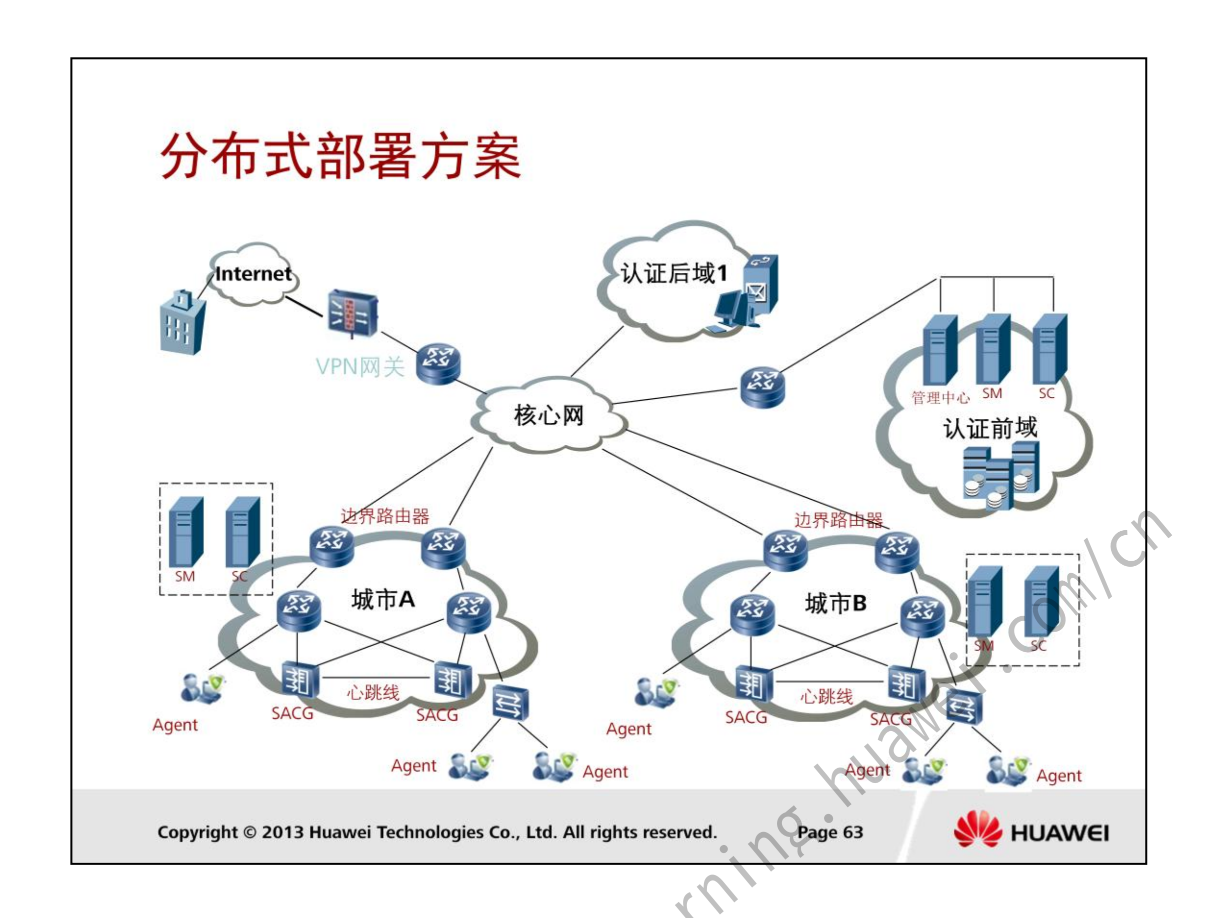
目录



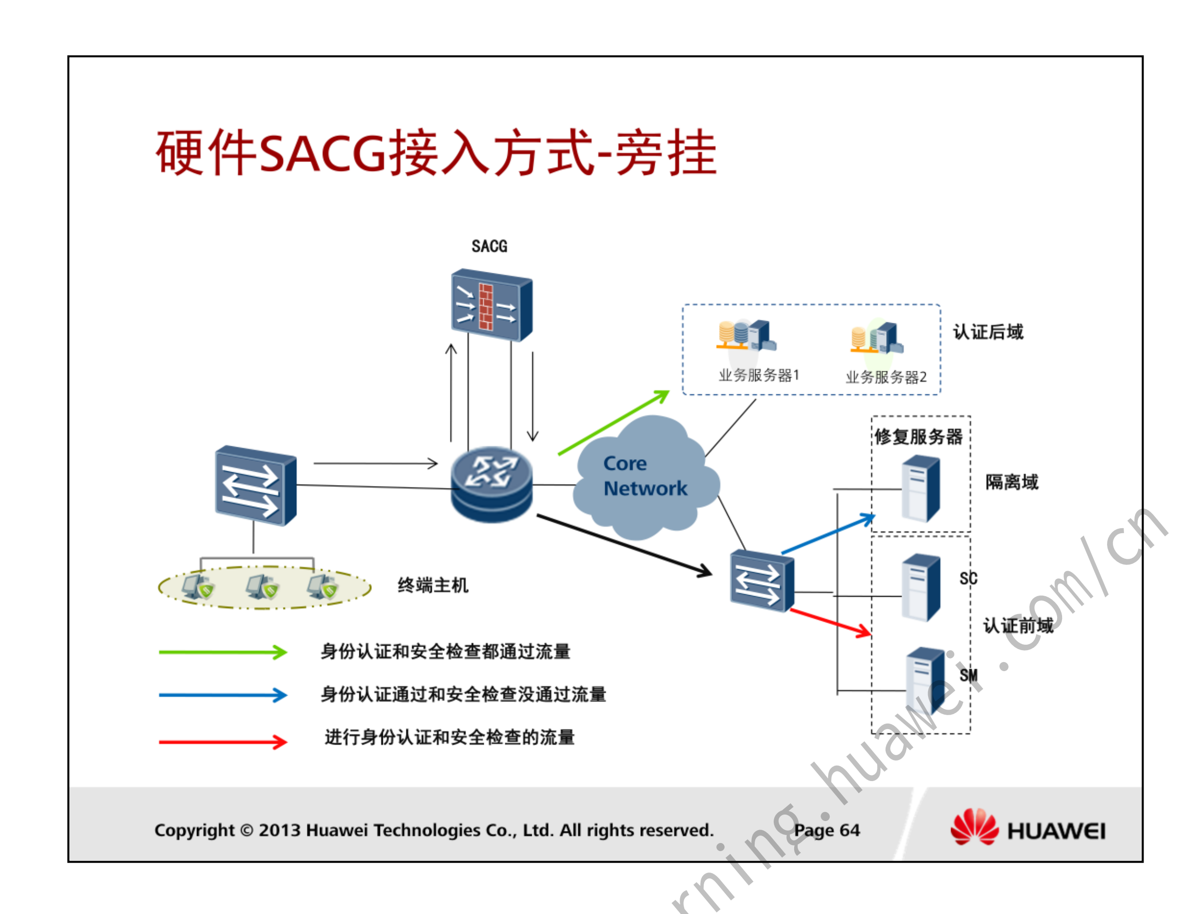


- 相关概念的介绍：
  - 认证后域：该区域放置企业核心信息资源，通过身份认证和安全检查的终端才可以访问的资源。
  - 隔离域：该区域放置补丁、病毒修复服务器，当终端通过了身份认证但是安全检查有问题时，可以访问该区域设备进行检查修复。
  - 认证前域：该区域放置终端安全系统，包括SC、SM、数据库等，终端可以自由访问该区域设备。

该方案在端点部署代理软件、企业内部路由器旁侧挂安全接入网关，在部署Secospace服务器就可实现Secospace的全面功能。SACG建议采用旁挂方式，不会影响现有网络拓扑结构，设用于中小型规模的网络。

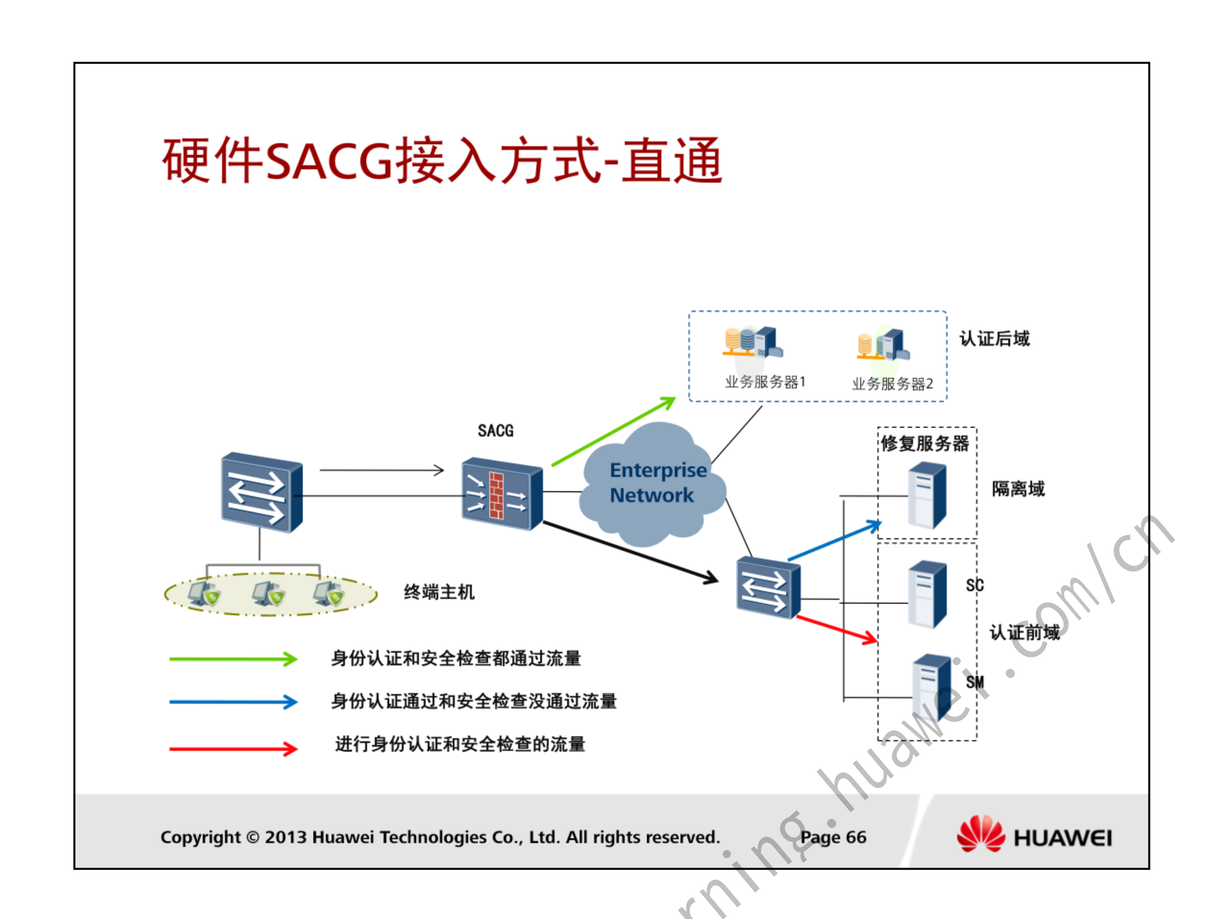


与小型组网相比，网络结构没有什么变化。但是大型组网中，在Secospace系统服务器方面，考虑到系统性能的问题，一般会采用多个SC服务器组成服务器集群，每个SC服务器负责特定地区的用户的身份认证和访问控制，有效地提高了系统的性能。同时在一个SM上统一负责对SC服务器进行集中管理，可以只使用一个安全修复服务器，因为所需要更新的安全信息和补丁都是一致的，另外，系统采用统一的数据库集群，所有的SC都与该数据库集群通信，进行数据的读取和更新操作，前面提过，虽然采用多个SC，但是数据是统一的。在大型组网中，SACG通常会采用双机热备分的方式，保证网络的可靠性，主备切换时能够保证业务不中断。

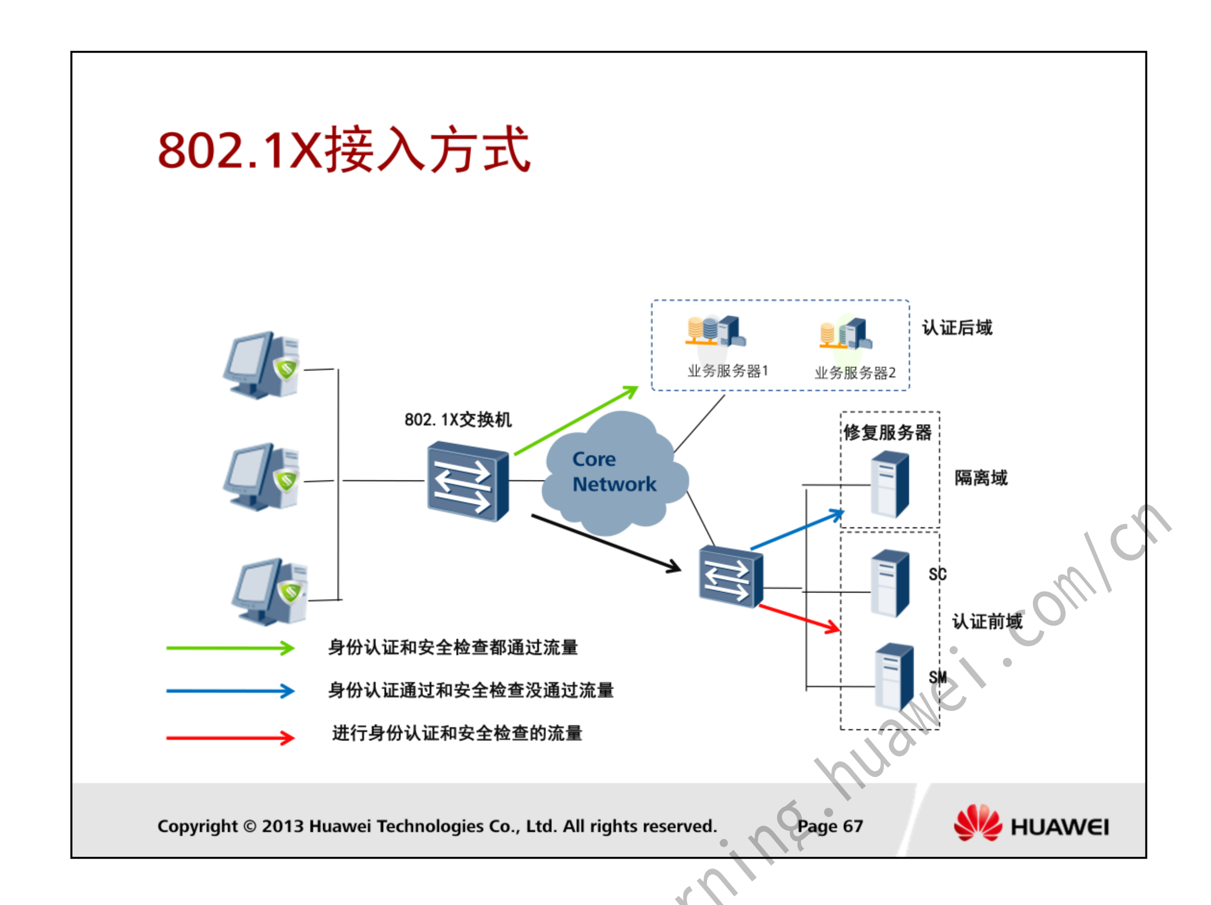


防火墙与终端安全系统联动，连接到控制器，向控制器请求同步认证前域的规则和认证后域的规则，把规则转换为ACL。其中认证前域对应1条ACL其编号为3099，每个受控域对应1对ACL。受控域对应的1对ACL由permit语句和deny语句组成，分别对应允许访问受控域和禁止访问受控域。

- 从交换机或路由器上接收数据流，并检查进入安全接入控制网关的报文。根据报文对应的IP地址的认证状态确定下一步如何处理；
  - 如果该IP地址未经过身份认证，安全接入控制网关将会使用认证前域对应的ACL对报文进行处理。该条ACL与管理员在SM管理器上配置的认证前域相对应；
  - 如果该IP地址已经通过身份认证，但未通过安全认证，硬件安全接入控制网关将该报文从认证前域切换至隔离域，并根据隔离域对应的ACL对报文进行处理。
  - 如果该IP地址同时通过身份认证和安全认证，硬件安全接入控制网关将该报文从认证前域或隔离域切换至认证后域，并根据认证后域对应的ACL对报文进行处理。



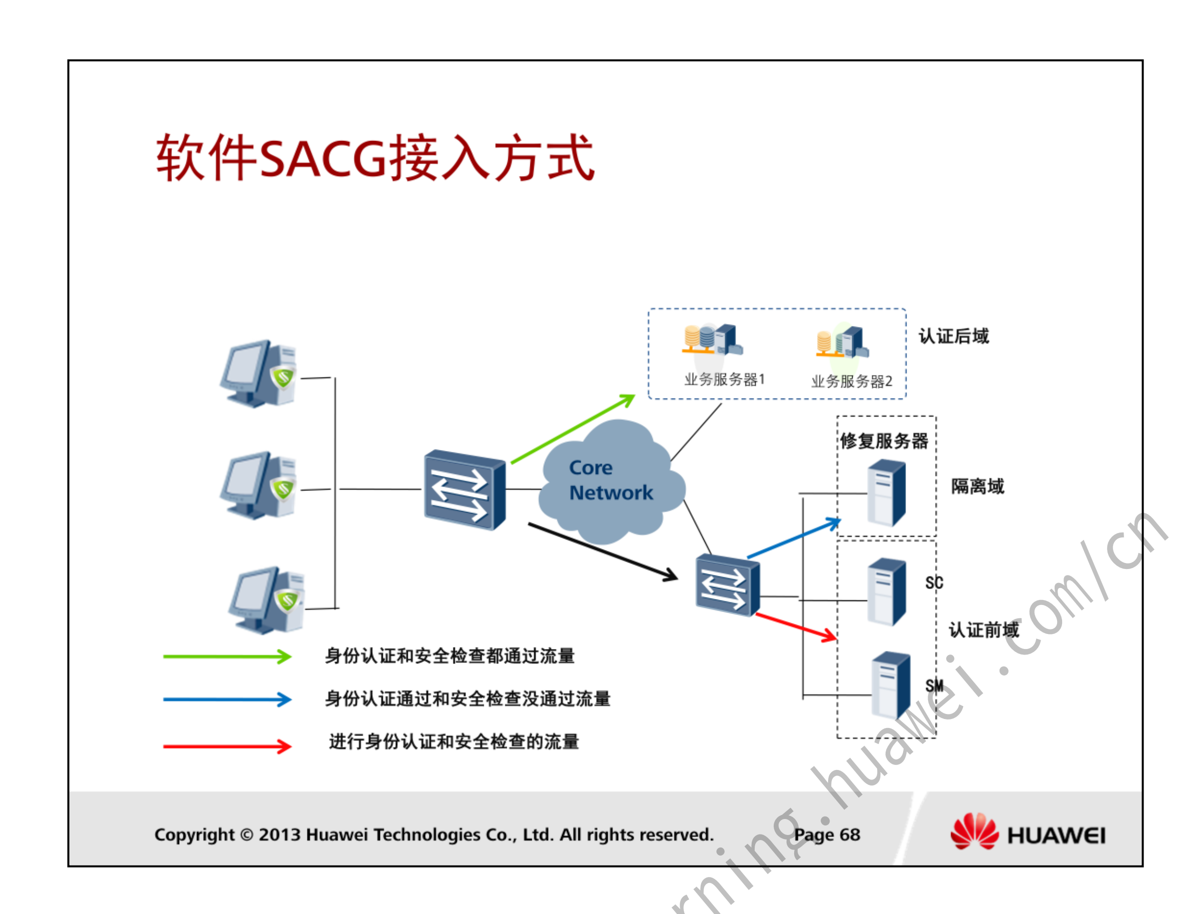
该方案的优点部署简单，易于维护，缺点是可能有单点故障风险,不适用于网络架构已经固定的场景，防火墙的接入控制的原理与旁挂方案相同。



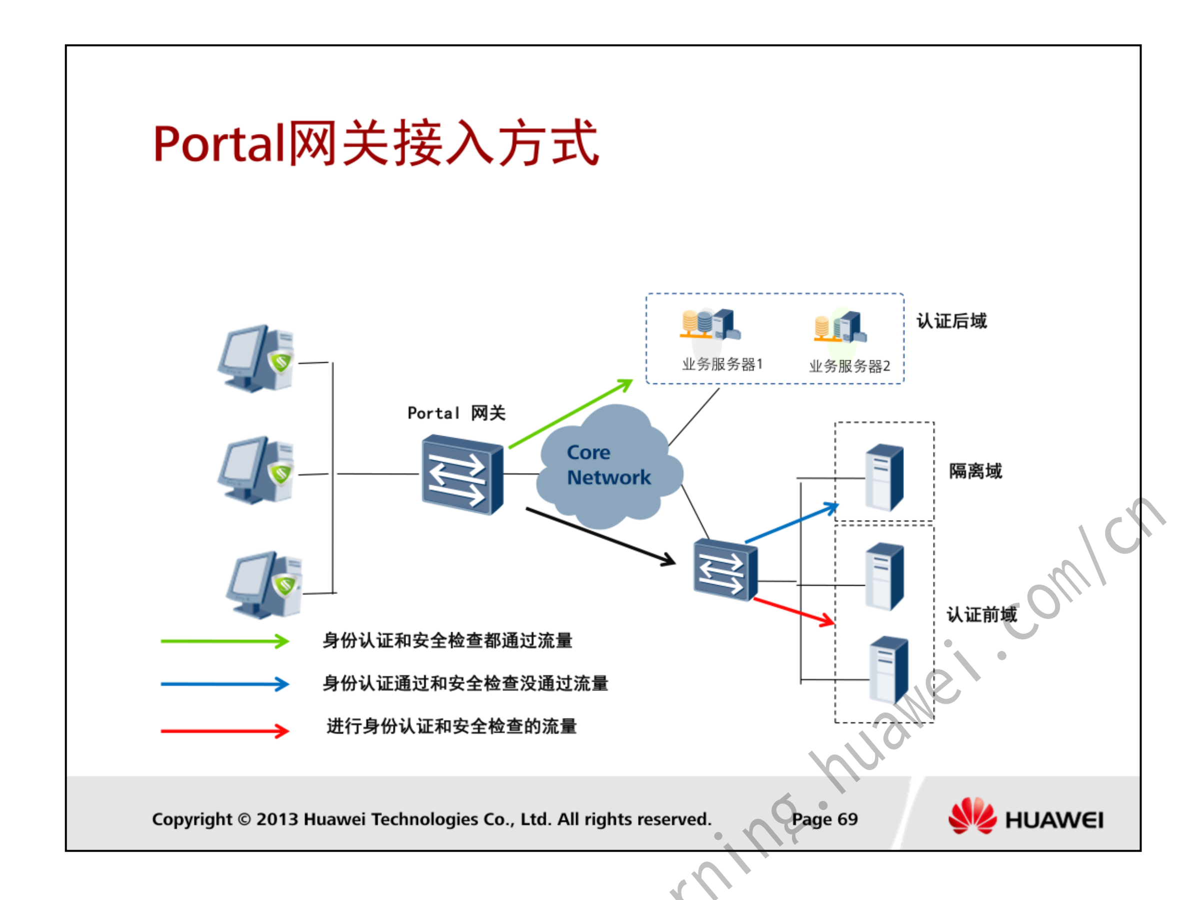
802.1x交换机的主要功能是对终端主机进行接入控制。通过端口控制技术，保证只有通过身份认证的终端主机才能接入受控网络，防止未经授权的终端主机接入受控网络。终端安全服务器对应于IEEE802.1x的认证服务器系统，用户接入层设备则实现IEEE802.1x的接入控制单元，IEEE802.1x的用户接入系统集成在代理中。

接入控制单元的每个物理端口内部有受控端口和非受控端口等逻辑划分。非受控端口始终处于双向连通状态，主要用来传递EAPOL协议帧，可保证随时接收用户接入系统发出的认证EAPOL报文。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

- 802.1x交换机对终端主机进行接入控制时：
  - 若终端用户已经通过身份认证和安全认证，则终端用户能够访问认证后域。
  - 若终端用户已经通过身份认证而未通过安全认证，则终端用户能够访问隔离域。
- 终端安全系统与802.1x交换机联动的方式有：
  - 基本的802.1x交换机接入控制
  - 基于动态VLAN的802.1x交换机接入控制
  - 基于动态ACL的802.1x交换机接入控制



软件SACG又成为主机防火墙，通过用户账号对终端进行接入控制，与硬件SACG相比，部署简单，易于维护，可以有效的控制主机之间的互访。



- 要判断终端主机的状态是否安全，终端用户的行为是否威胁网络安全，要视策略的执行结果而定。通过在Portal认证报文中携带安全检查结果，交换机将安全检查结果作为终端主机接入受控网络的判断因素之一：
    - 如果终端用户未能通过身份认证，则终端用户只允许访问不受限的网络资源。
    - 如果终端用户通过身份认证，但安全检查出现严重违规，并且管理员启用严重违规拒绝终端主机接入网络，则终端主机被隔离，只允许访问有限的网络资源帮助消除违规信息，无法访问受限的网络资源。
    - 如果终端用户通过身份认证，并且管理员未启用严重违规拒绝终端主机接入网络，则允许终端用户访问受限的网络资源。
    - 如果终端用户同时通过身份认证和安全检查，则允许终端用户访问受限的网络资源。
- Portal网管对终端主机进行接入控制：
    - 若终端用户已经通过身份认证和安全认证，Raduis服务器下发后域ACL给Portal网关，则终端用户能够访问认证后域。
    - 若终端用户已经通过身份认证而未通过安全认证，Raduis服务器下发隔离域ACL给Portal网关，则终端用户能够访问隔离域。
- 为了完成安全检查任务，终端主机必须安装代理或Web Agent插件。在身份认证通过而安全检查不通过的情况下，终端主机将会被隔离，修复违规后再次尝试认证。同时通过身份认证和安全检查的终端主机才能访问网络中的受限网络资源。
- 如果不安装代理或Web Agent插件，只使用Web客户端，则Portal认证只具有身份认证功能，不具备安全检查功能。故在使用Web客户端进行认证的情况下，无法达到隔离安全检查出现严重违规的终端主机。终端用户通过身份认证后不执行安全检查，直接获取权限访问受限网络资源。



目录

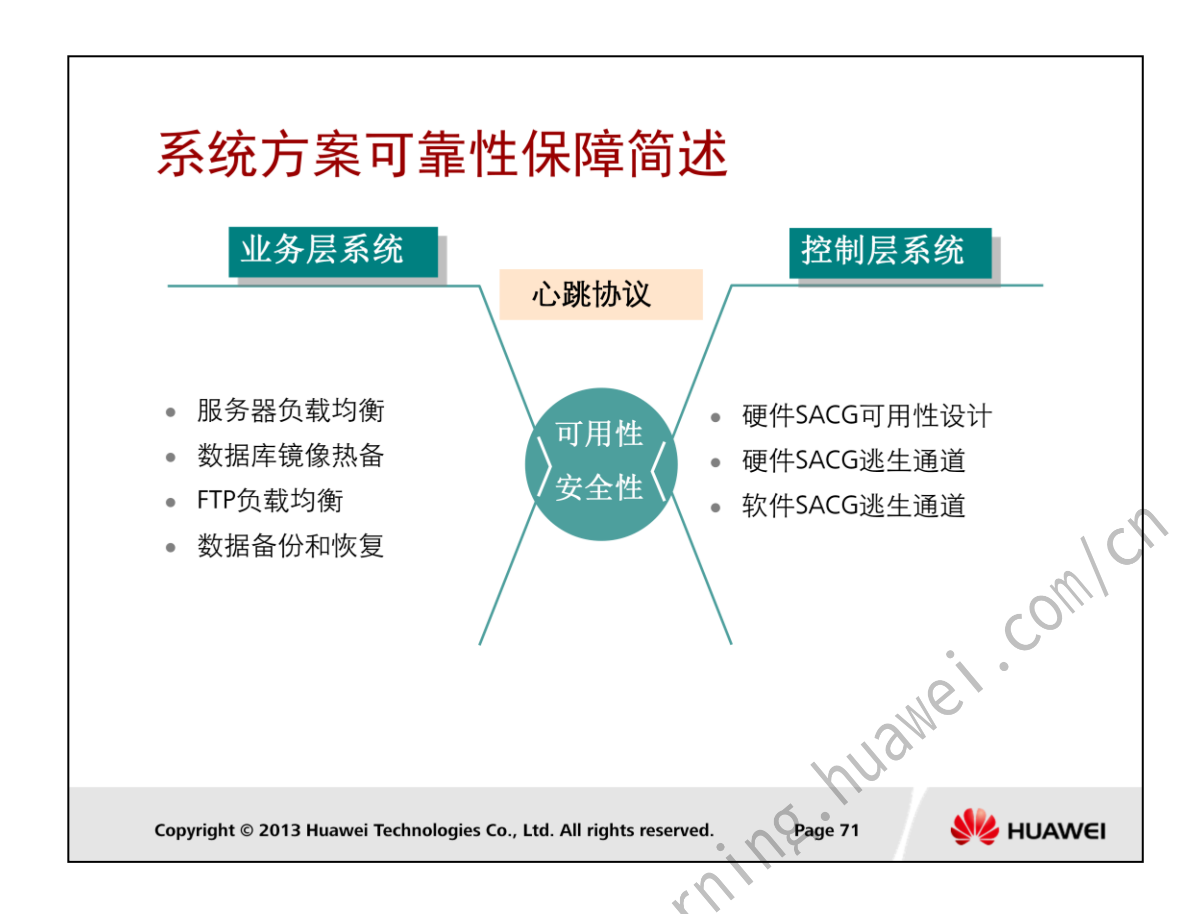
1. 终端安全设计思想概述
2. 终端安全技术
3. Policy center 系统简介
4. **终端安全系统设计**

   4.1终端安全系统设计概述

   4.2 组网方案设计

   4.3 可靠性设计

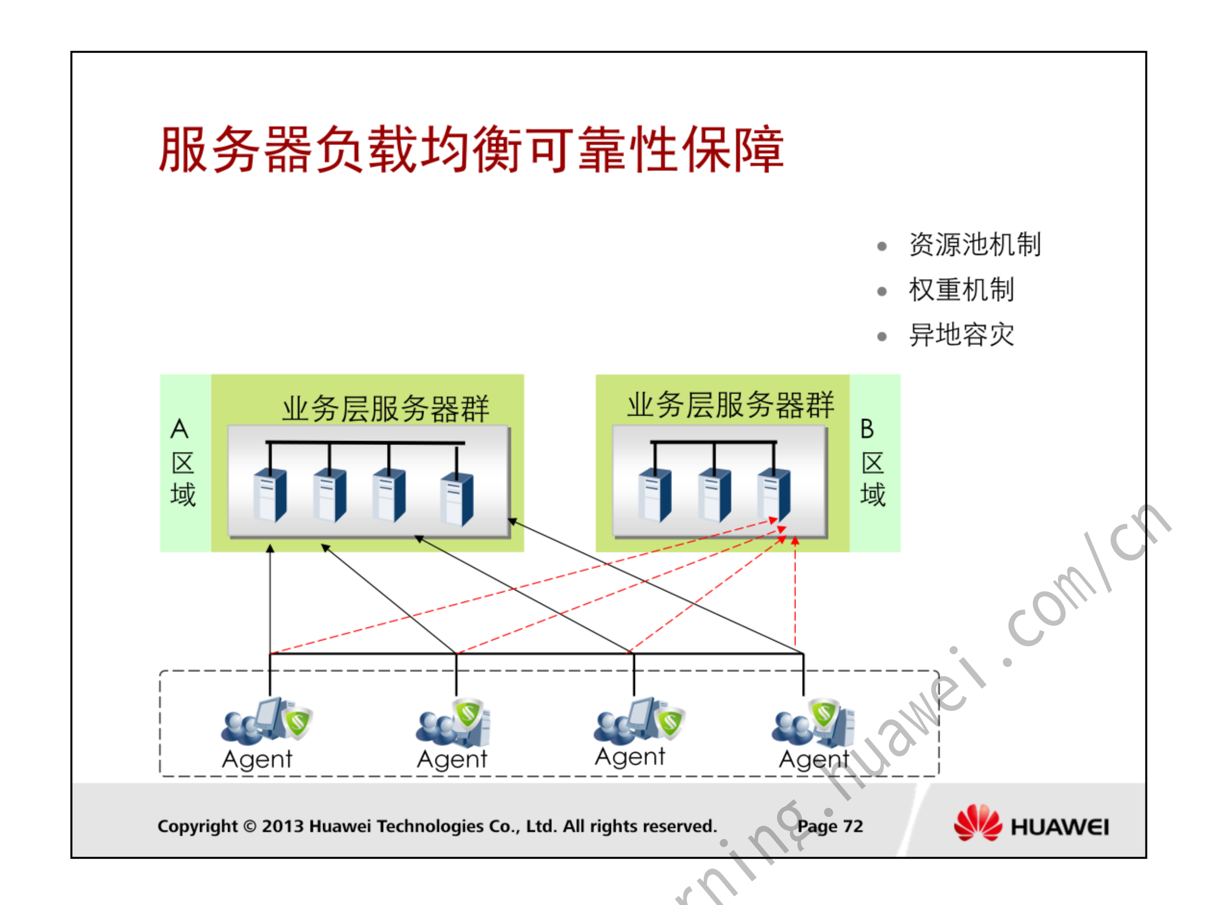




系统方案可靠性保障共分为业务层系统和控制层系统，这2个系统的可靠性保障有部分实现是采用心跳协议，且在某些情况下需做好可用性和安全性之间的平衡。

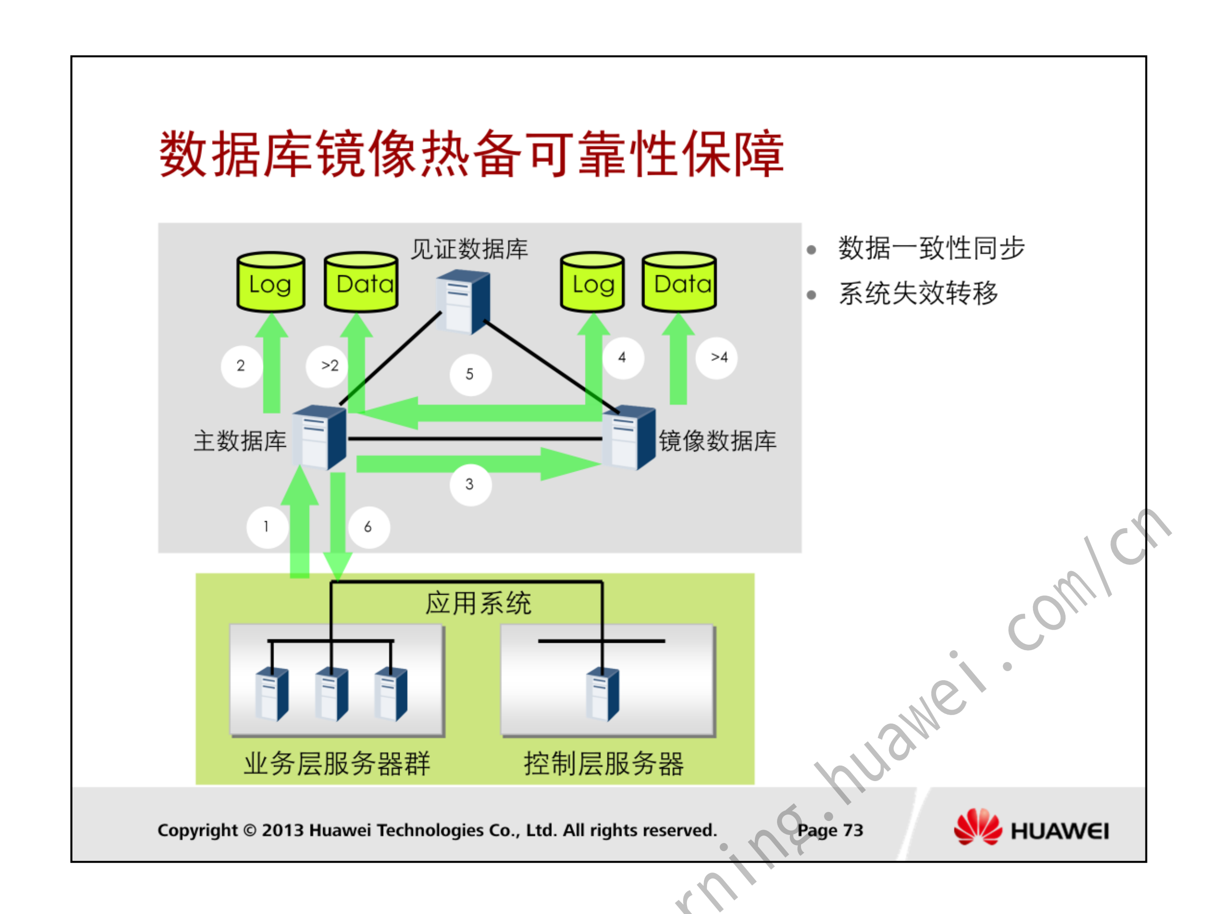
在业务层系统方面，支持服务器负载均衡、数据库镜像热备、FTP负载均衡、数据备份和恢复等；在控制层系统方面，支持硬件SACG双机热备、硬件SACG逃生通道、软件SACG逃生通道等。

- 逃生通道：它通过业务层系统和控制层系统之间的心跳协议进行定期交互，若在指定时间内未收到心跳报文，控制层系统将开启逃生通道功能，以支持业务的可用性，但降低了安全性；
- 失效转移：在服务器负载均衡环境，一般情况下所有服务器共同承担终端用户的交互业务，当某中某台服务器发生故障后，终端用户将进行失效转移功能，以保障业务的连续性；
- 数据备份和恢复：在所有数据库均发生故障的情况下，可以利用恢复工具把之前备份的数据恢复回来，比如用户信息、密钥、策略模板等。



服务器负载均衡有2种主要的实现机制：资源池机制和权重机制。资源池机制即是所有服务器都是平等，终端用户将获取所有服务器群IP地址，然后根据算法随机一台服务器做为后续业务的交互对象；而权重机制而是对每台服务器设置一个值(0-100之间)，终端用户连接某台服务器的概率与权重有关。权重越大，终端用户将与其进行业务交互的机会越大；反之，权重越小，终端用户将与其进行业务交互的机会越小。因此，权重设置相同的机制与资源池机制一致。

异地容灾：服务器负载均衡可根据企业对可用性的特别要求，提供异地容灾功能。比如当A区域某台服务器发生故障，终端用户的业务交互将全部转向其它服务器。但如果其它服务器也无法支撑当前所有终端用户的业务请求（性能出现瓶颈）或A区域所有服务器均发生故障（或网络中断），这时终端用户可把业务交互请求发向B区域指定的备用业务层服务器。



数据库镜像热备可靠性保障，通过主数据库、镜像数据库、见证数据库服务器实现数据一致性同步和系统失效转移。所有应用系统在同一时间只与其中一台数据库服务器进行业务交互，即与主数据库服务器，当主数据库服务器发生故障后，所有应用系统将把业务切换到镜像数据库服务器，而此时镜像数据库服务器也提升为主数据库服务器。

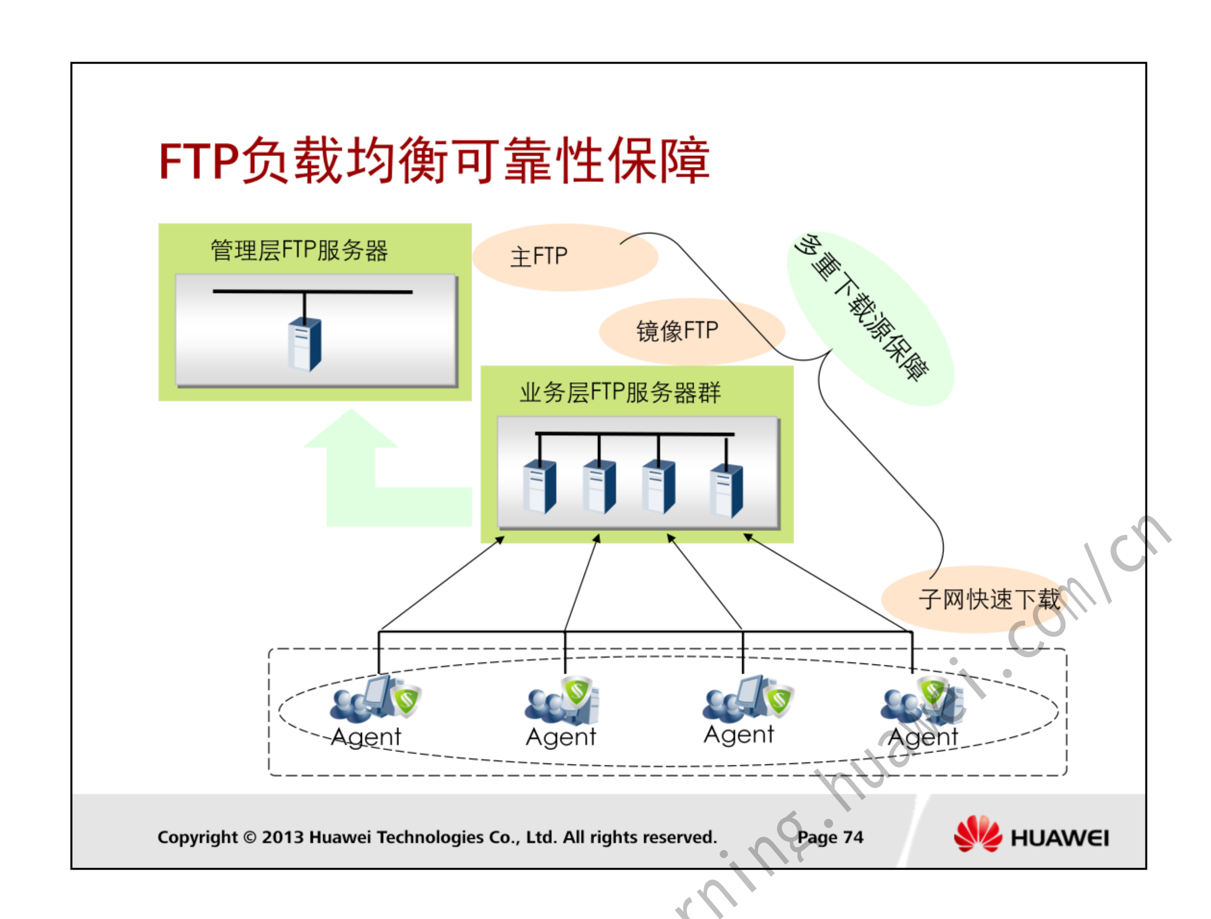
数据一致性同步：在应用系统写入数据至数据库时，首先先把数据写入主数据库，然后再写入镜像数据库，在完成镜像数据库写入后，才把写入成功信息反馈给应用系统，从而保障主数据库服务器与镜像数据库服务器数据始终统一；

系统失效转移：在主数据库正常运行中，应用系统只与主数据库服务器进行业务交互。当主数据库服务器发生故障后，应用系统将自动转移与镜像服务器进行业务交互，而此时镜像数据库服务器也提升为主数据库服务器。

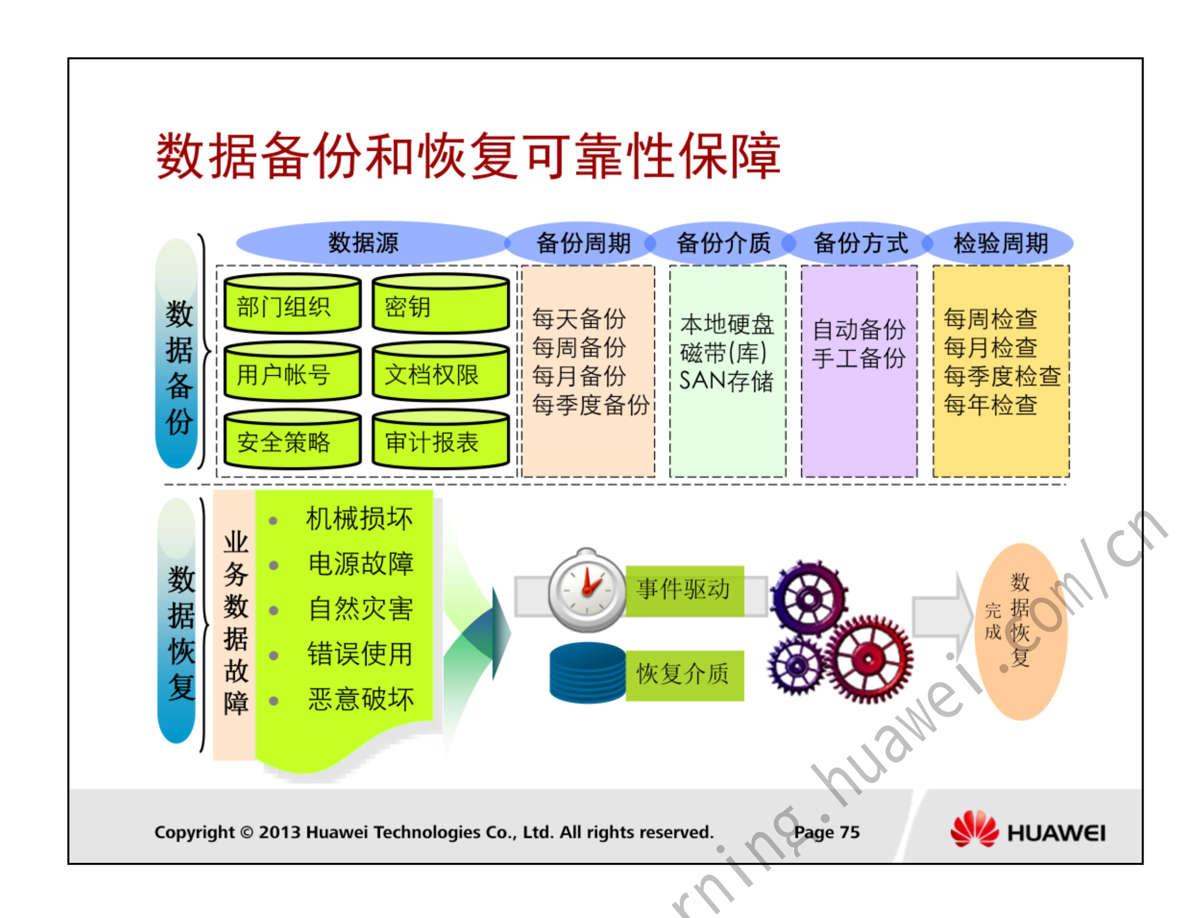
见证数据库是独立于主数据库、镜像数据库的第3个Microsoft SQL Server 2005数据库实例。见证数据库用来判断在什么情况下需要进行数据错误恢复。

在主数据库和见证数据库同时崩溃的情况下，镜像数据库是不允许访问的。这时管理员需要先停止镜像数据库，然后将镜像数据库的数据库文件和数据库日志文件剪切到其他地方，接着启动镜像数据库，在删除镜像数据库后，再通过附加文件的方式将数据库文件和数据库日志文件恢复至数据库中。

数据库镜像必须具备三台硬件服务器，每台硬件服务器均安装了Microsoft SQL Server 2005，Microsoft SQL Server 2005在三台硬件服务器上的安装路径完全一致，并且安装了Microsoft SQL Server 2005 SP3补丁。

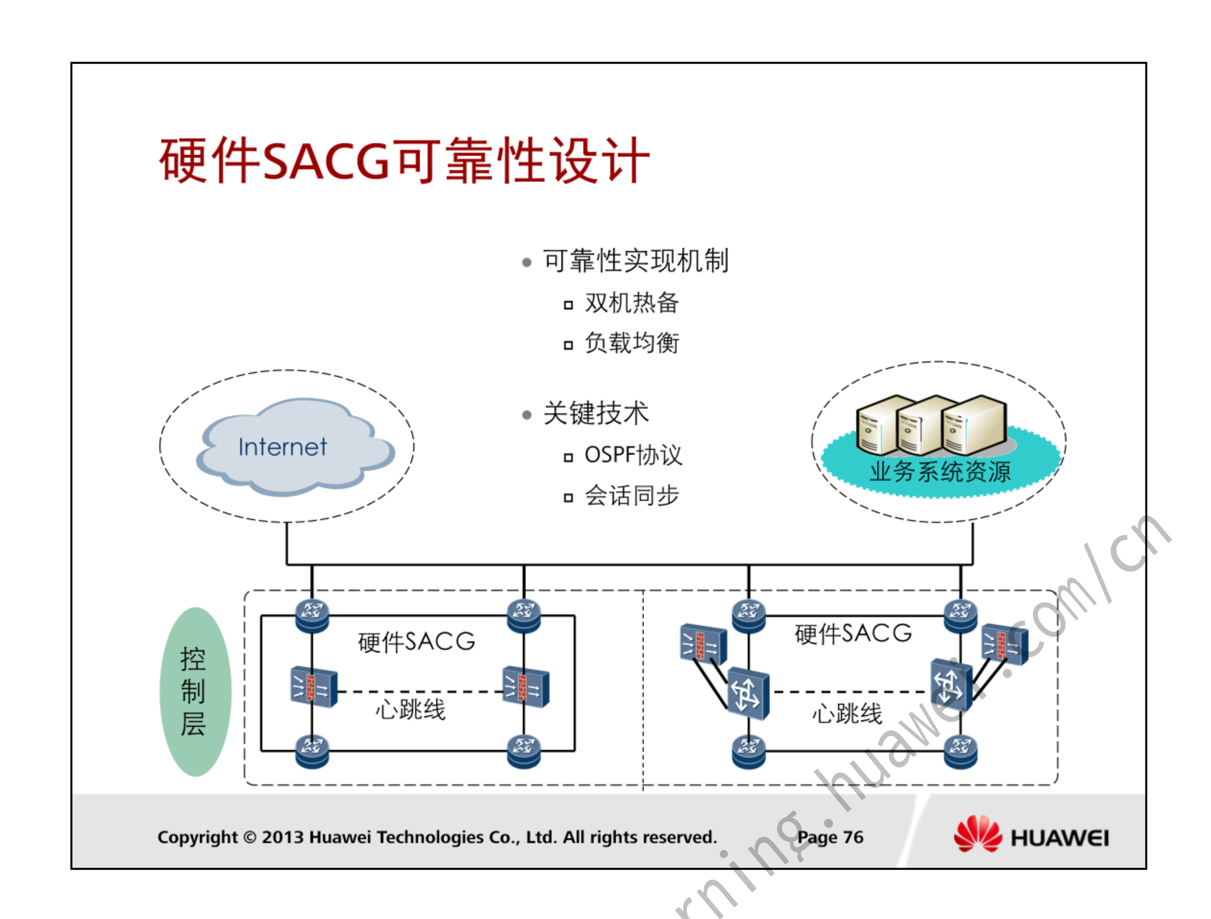


在业务系统资源保障部分，需通过获取补丁、软件等来实现企业信息安全基线要求。需获取以上信息最好的途径主要有子网下载和FTP下载2种主要方式，在终端安全方案中，主要通过提供子网下载镜像FTP下载、主FTP下载 3 种手段来保障有效地信息获取，即任何一种手段发生问题，均有其它手段进行补充，以保障业务开展的连续性。

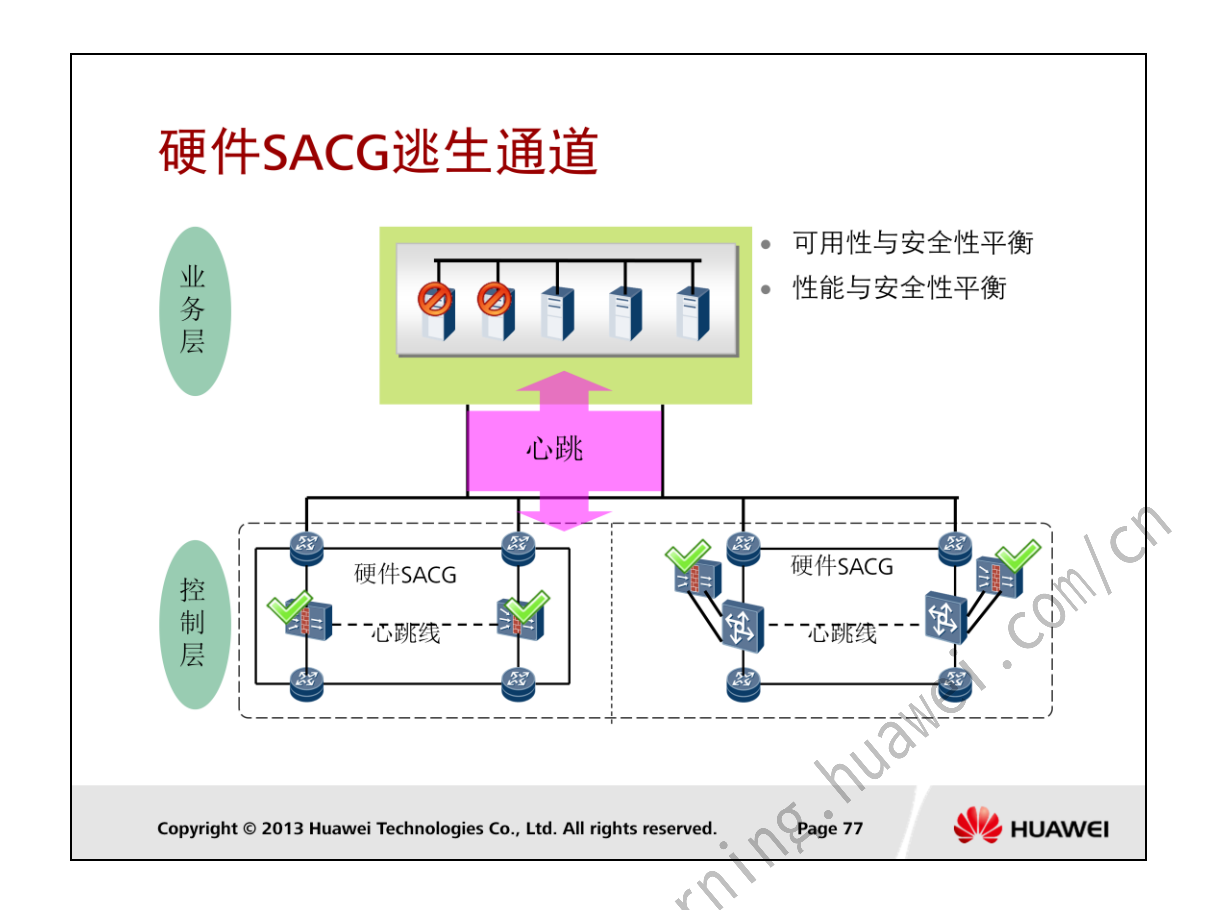


终端安全系统方案的数据主要包括部门组织、用户帐号、安全策略、密钥、文档权限、审计报表等，且存储在主流的数据库系统，如MS SQL 2005中。以下将以MS SQL 2005做为样本进行阐述。若要保障数据备份的正常运行，需开启SQL Server Agent自启动功能，便于在操作系统启动时，其也处于启动状态。

- 在数据恢复方面，业务数据故障主要存在以下5项：
  - 机械损坏：计算机的各种部件(包括磁盘)都存在机械故障可能性；
  - 电源故障：指UPS无法保护的异常电源故障；
  - 自然灾害：地震、水灾、火灾或其他原因造成的严重故障；
  - 错误使用：应用程序以及服务程序在使用中的中途故障，导致数据不完整；
  - 恶意破坏：一些恶意破坏者对数据库执行非法的篡改数据、删除数据操作。

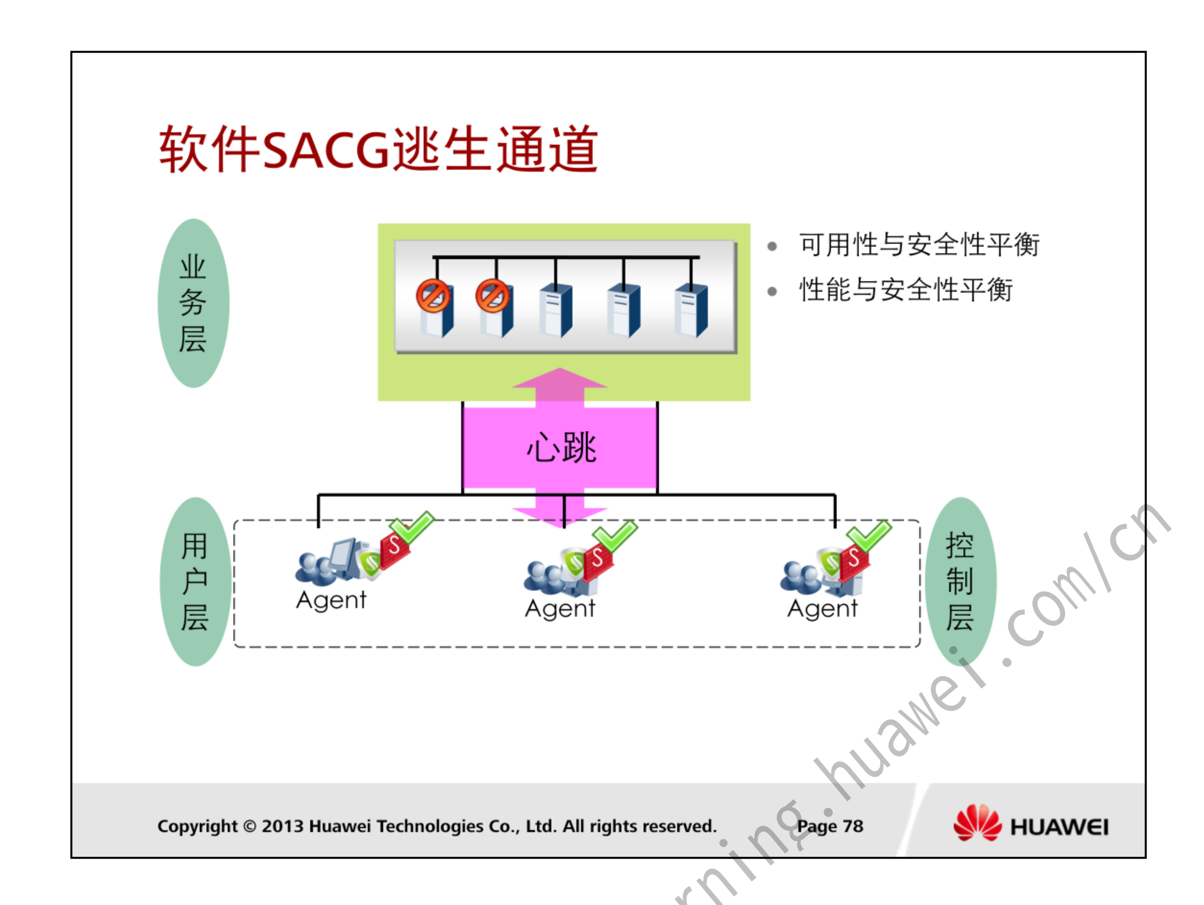


在负载均衡情况下，需配置”会话快速备份“来实现会话能及时向另一台网关同步。



- 可用性与安全性平衡:
  - 在可用性比安全性更重要场景，逃生通道是比较有效的解决方案。硬件SACG定期与业务层服务器保持心跳协议，当在一定周期内与业务层服务器心跳报文中断，硬件SACG将开启逃生通道开关（放开所有业务，不对终端用户的接入进行控制），以保障业务的连续性。
- 性能与安全性平衡:
  - 为了保证所有的终端用户能正常地进行业务操作，业务层服务器的数量要能支撑现有终端用户的业务请求性能，避免因性能问题（业务层服务器故障达到一定数量，将使整体业务层响应请求受影响）导致部分终端用户无法通过认证，从而业务中断。因此，当有效的业务层服务器达到一定数量后，硬件SACG将开启逃生通道功能。

备注：当业务层服务器恢复工作后，逃生通道将关闭，终端安全系统将又处于安全控制之下。



- 可用性与安全性平衡：
  - 在可用性比安全性更重要场景，逃生通道是比较有效的解决方案。软件SACG定期与业务层服务器保持心跳协议，当在一定周期内与业务层服务器心跳报文中断，软件SACG将开启逃生通道开关（放开所有业务），以保障业务的连续性。
- 性能与安全性平衡：
  - 为了保证所有的终端用户能正常地进行业务操作，业务层服务器的数量要能支撑现有终端用户的业务请求性能，避免因性能问题（业务层服务器故障达到一定数量，将使整体业务层响应请求受影响）导致部分终端用户无法通过认证，从而业务中断。因此，当有效的业务层服务器达到一定数量后，软件SACG将开启逃生通道功能。
- 备注：当业务层服务器恢复工作后，逃生通道将关闭，终端安全系统将又处于安全控制之下。



总结

1. 终端安全设计思想?
2. 接入控制技术有哪些?
3. Policy center 系统主要功能?
4. 如何保证终端安全系统的可靠性?





思考题

- 在终端安全系统中FTP服务器的功能和作用是什么?
- 可靠性中SACG双机热备和负载均衡如何部署及配置?
- 硬件SACG接入控制方式部署终端安全系统，终端通过身份及安全认证后可以访问隔离域吗?





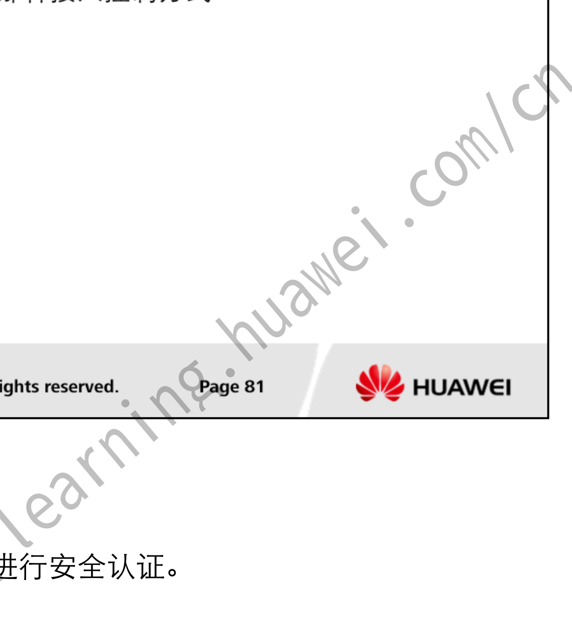
- 判断题
  1. Web网页认证可以对终端进行安全认证。
- 单选题
  1. 可以有效控制终端间互访的是那种接入控制方式?

     A.硬件SACG

     B.软件SACG

     C.802.1X接入控制

     D.Portal网关



- 习题与答案:
  - 判断题：Web网页认证可以对终端进行安全认证。

    答案：错误
  - 单选题：可以有效控制终端间互访的是?

    A.硬件SACG

    B.软件SACG

    C.802.1X接入控制

    D.Portal网关

    答案：B

Thank you

www.huawei.com

HC120320003 终端安全系统的安装和部署

www.huawei.com

HUAWEI



目标

- 学完本课程后，您将能够:
  - 掌握终端安全系统的安装；
  - 掌握终端安全系统的部署方案及要求；
  - 掌握终端安全系统各种场景的部署操作；



本章介绍了终端安全系统的安装。

- 重点关注:
  - 安装
  - Policy center的部署



目录

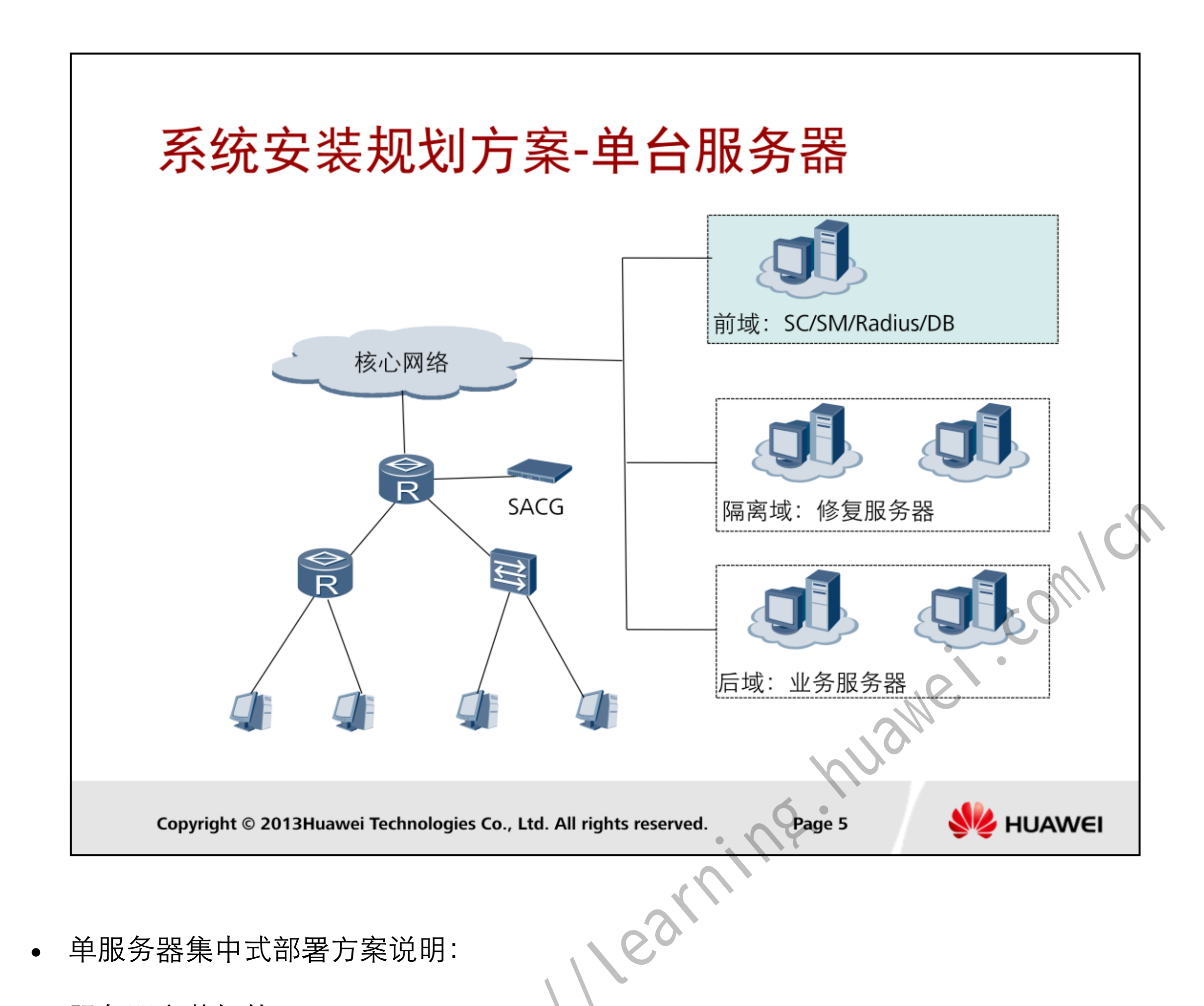
本节主要介绍终端安全系统的安装部署



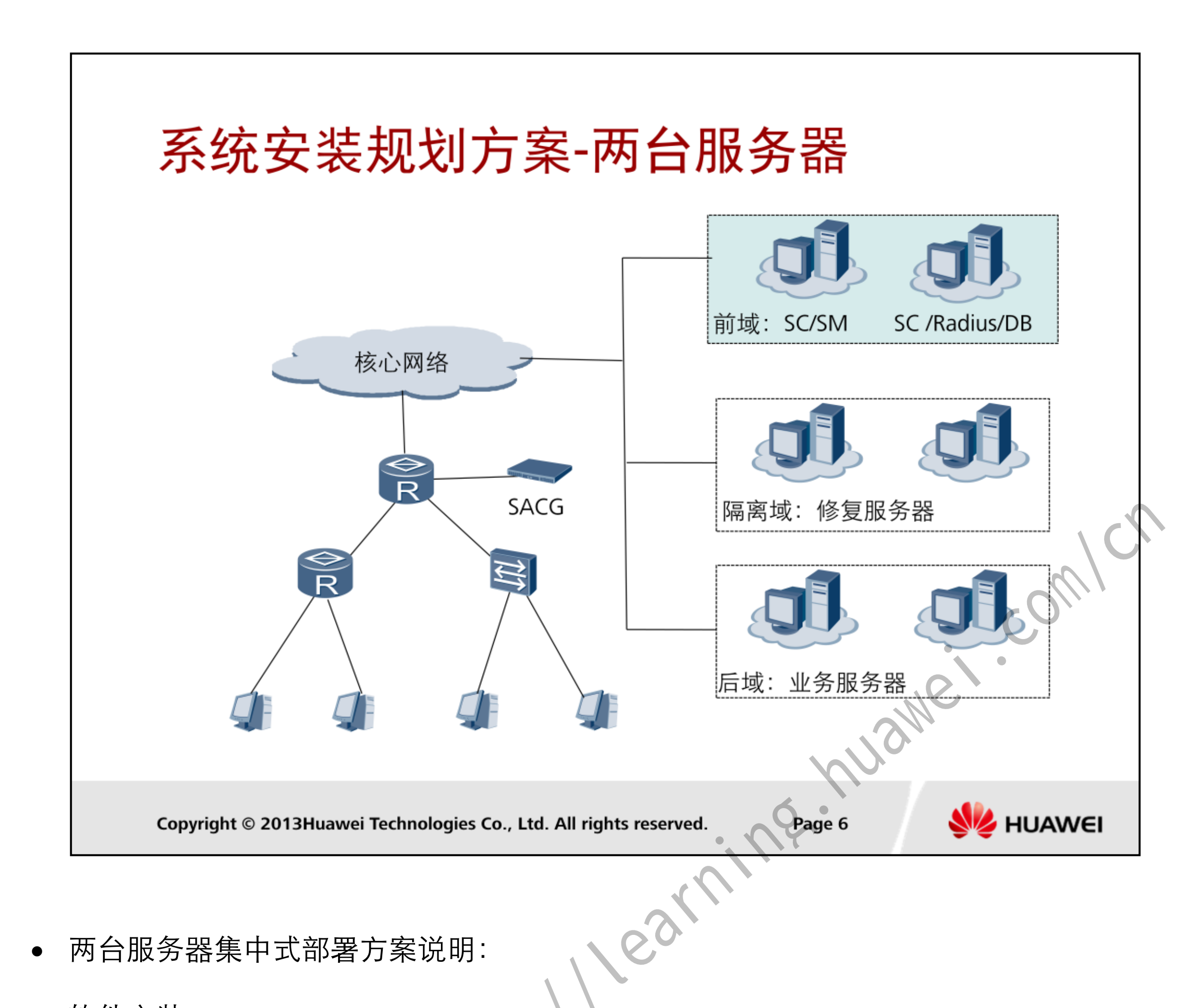
目录



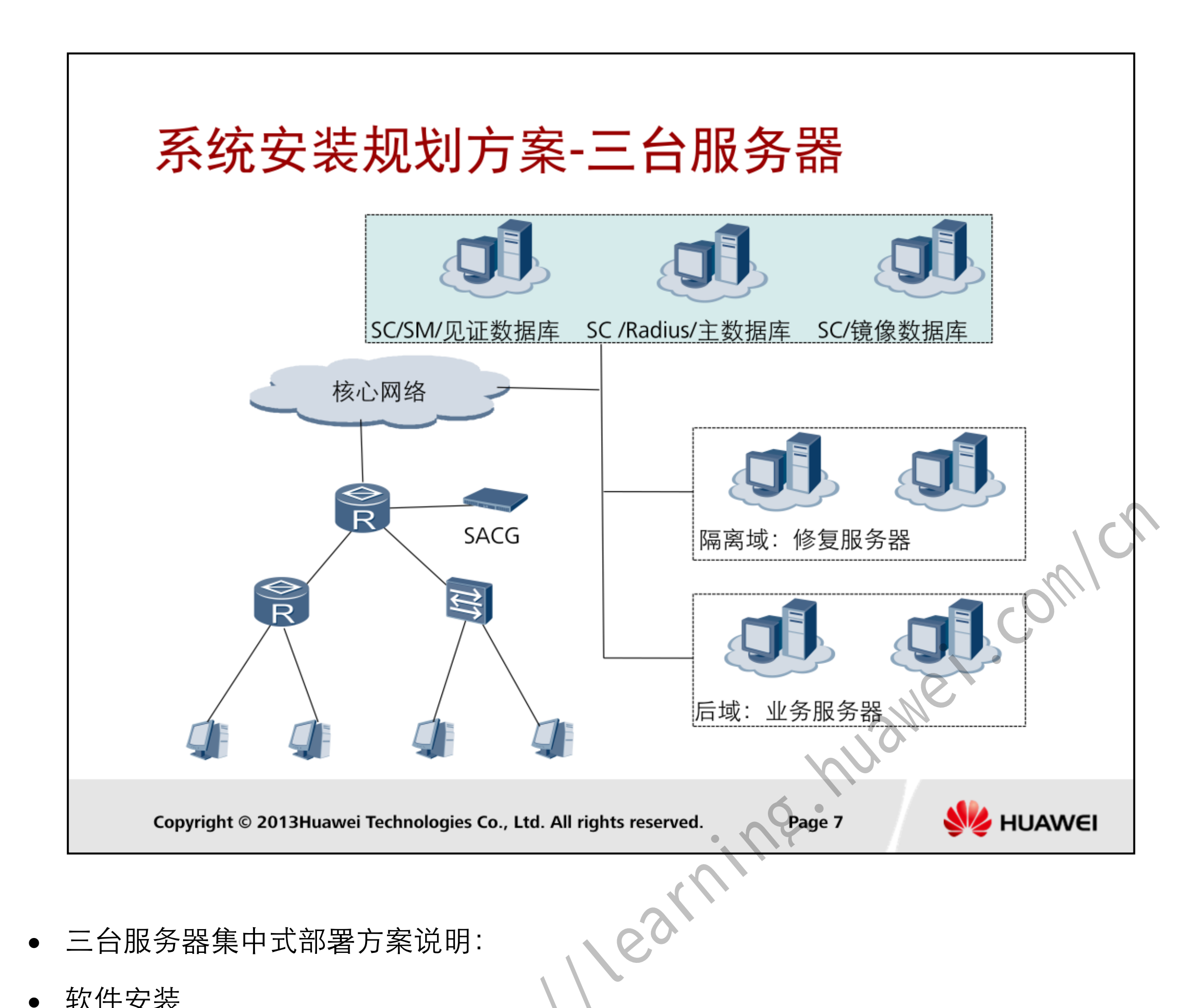
本节主要介绍终端安全系统的安装部署



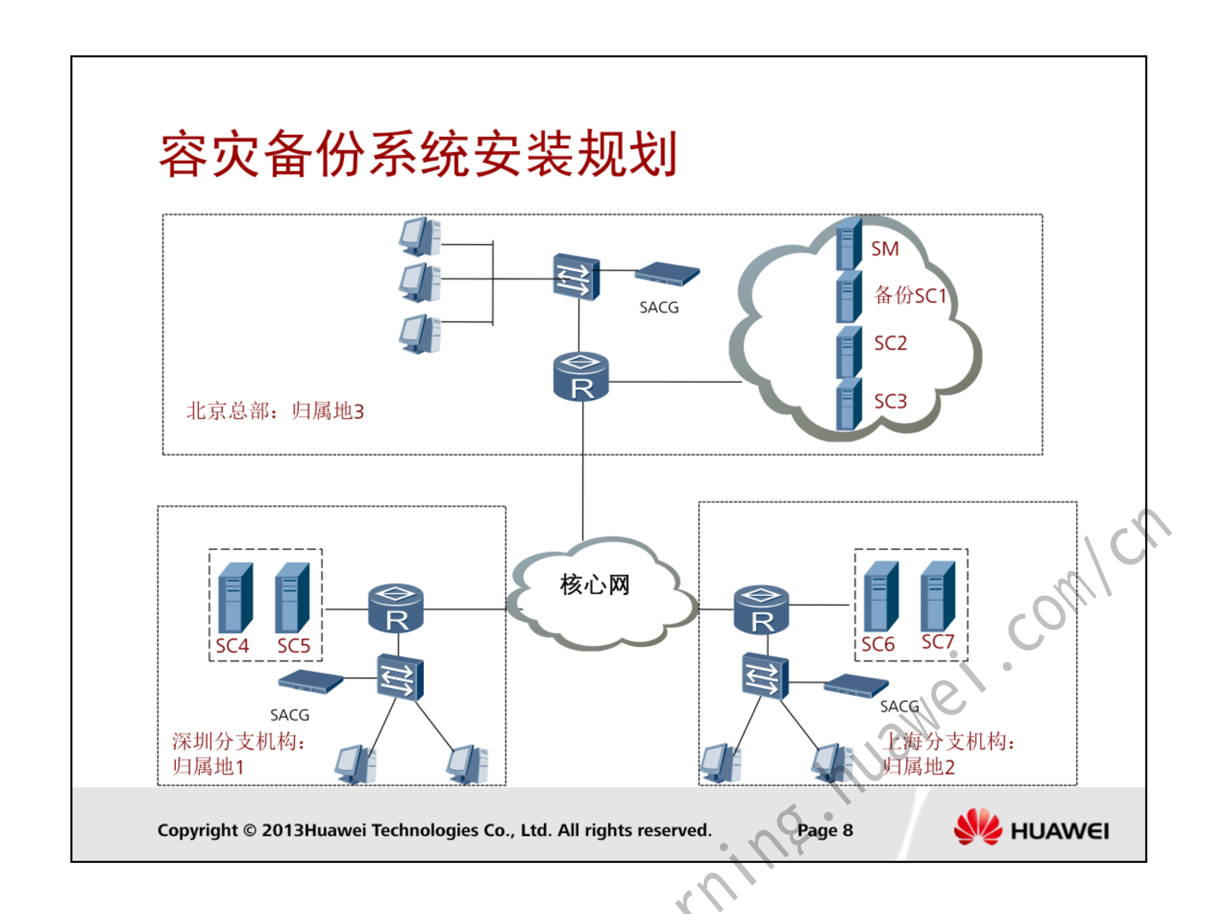
- 单服务器集中式部署方案说明：
- 服务器安装组件
  - 数据库，管理服务器SM，控制服务器SC、RADIUS服务器、FTP服务器
- 建议：
  - 建议单服务器集中组网时，被管理终端的数量小于2000
  - 当终端数量大于2000终端时，网络的规模已经比较大，对可靠性的要求会更高，虽然一个控制服务器SC能够管理1万终端，但是从可靠性的角度考虑，不推荐使用该方案
- 局限性：
  - 无法提供数据库热备功能
  - 只能部署一个控制服务器SC，无法提供控制服务器失效转移功能，当控制服务器SC发生故障的时候，无法提供终端的身份认证和准入控制等基本服务



- 两台服务器集中式部署方案说明:
- 软件安装
  - 服务器1安装组件：管理服务器SM、控制服务器SC 、FTP服务器
  - 服务器2安装组件：控制服务器SC、RADIUS服务器、数据库DB、FTP服务器
- 建议:
  - 建议双服务器集中组网时，被管理终端的数量小于10000
  - 当终端数量大于10000终端时，网络的规模已经非常大，对可靠性的要求会更高，虽然一个控制服务器SC能够管理1万终端，两个服务器能够支撑20000终端，但是从可靠性的角度考虑，1万终端以上的网络不建议使用该方案
- 局限性:
  - 无法提供数据库热备功能



- 三台服务器集中式部署方案说明：
- 软件安装
  - 服务器1安装组件：管理服务器SM、控制服务器SC 、见证数据库、FTP
  - 服务器2安装组件：控制服务器SC、FTP、主数据库
  - 服务器3安装组件：控制服务器SC、FTP、镜像数据库
- 建议：
  - 当终端数大于20000终端时，没有现成的方案，需要市场技术与研发一同评估后提供



该种部署场景是在区分地域的负载分担基础上，增加备用控制器，确保当某个归属地的所有控制器出现故障无法连接时，客户端能够连接备用控制器完成认证。为了提高控制器的可靠性，便于管理员对辖区范围内的控制器进行维护和管理，管理器为每台控制器定义位置属性，称之为归属地，用于表示控制器所在的位置,地址池是指由管理器统一管理某一个归属地的所有主用控制器和备用控制器的一种机制。当该归属地的控制器出现工作负荷过大或者出现故障时，管理器将接入控制业务自动切换至同一归属地的其他可用控制器，确保网络不会被中断。未分配任何控制器的归属地称之为无效归属地。如果代理选择的归属地为无效归属地，则终端用户无法接入受控网络。

当出现故障的控制器中的一台恢复正常后，客户端立即从连接备用控制器切换到连接恢复正常的控制器

- 举例：某公司总部在北京，在上海、深圳设置了分支机构。为了实现负载分担和容灾备份，各个分支机构部署了多台控制器，并在北京部署了备用控制器SC1，则在部署时管理员需要在管理器完成以下工作： 添加各个分支机构包括的所有控制器（包括备用控制器）。
  - 创建归属地北京、上海和深圳。
  - 在各个归属地的“SC地址池”中添加各归属地的控制器，并在“备SC地址池”中添加备用控制器。在归属地北京的“SC地址池”中添加分支机构北京包括的所有控制器，并在“备SC地址池”中添加备用控制器。
  - 部署完成后，各地员工在进行认证时，NAC Agent客户端会从对应的归属地的地址池中随机选择一台控制器进行连接。当某个归属地的所有控制器出现故障不可用时，客户端会自动切换到备用控制器进行认证。

磁盘分区及安装路径规划

- 服务器磁盘分区规划

推荐使用3*300G的硬盘（或者5*146G的硬盘），做RAID5

分区名称	说明
C盘	C盘的大小=100G，文件格式为NTFS
D盘	D盘的大小等于剩余磁盘空间，文件格式为NTFS

- 软件推荐安装路径

软件	安装路径
Windows Server 2003 Windows Server 2008 R2	C盘
SQL Server 2005 SQL Server 2008	D:\MSSQLSERVER
Policy Center软件	默认路径
FTP SERVER	D:\FTP
设备扫描器	默认路径

为了防止单块硬盘损坏导致数据丢失，按照服务器标准配置，可采用5块硬盘组成RAID5（Redundant Array of Independent Disks）方案，每块硬盘146GB，分成2个磁盘分区。



目录

1. 终端安全系统的安装
    1.1 安装规划
    1.2 数据库的安装
    1.3 Policy center的安装
    1.4 NAC Agent的定制
2. Policy Center系统配置
3. 终端安全系统部署



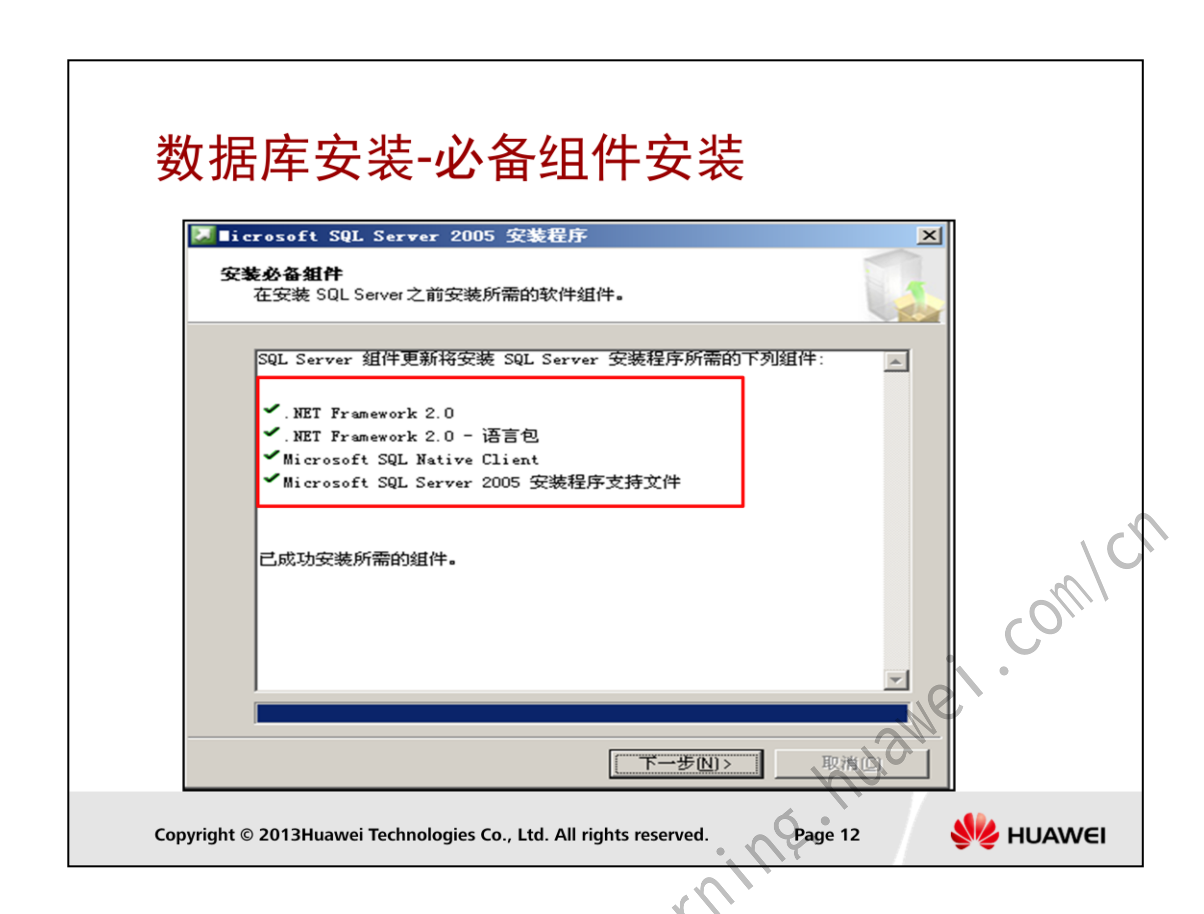
本节主要介绍终端安全系统数据库安装。

安装数据库准备

- 检查硬件服务器的软硬件配置是否符合最低要求：
  - OS：Windows Server 2003标准版\企业版，已经安装SP2补丁或者Windows Server 2008标准版\企业版
  - CPU：2*E5504
  - 内存：4G
- SQL SERVER 2005光碟/程序和SQL SERVER 2005 SP3光碟/程序
- 确保1433端口处于未被占用状态
  - 如果1433端口已被其他应用程序占用，先停止该应用程序



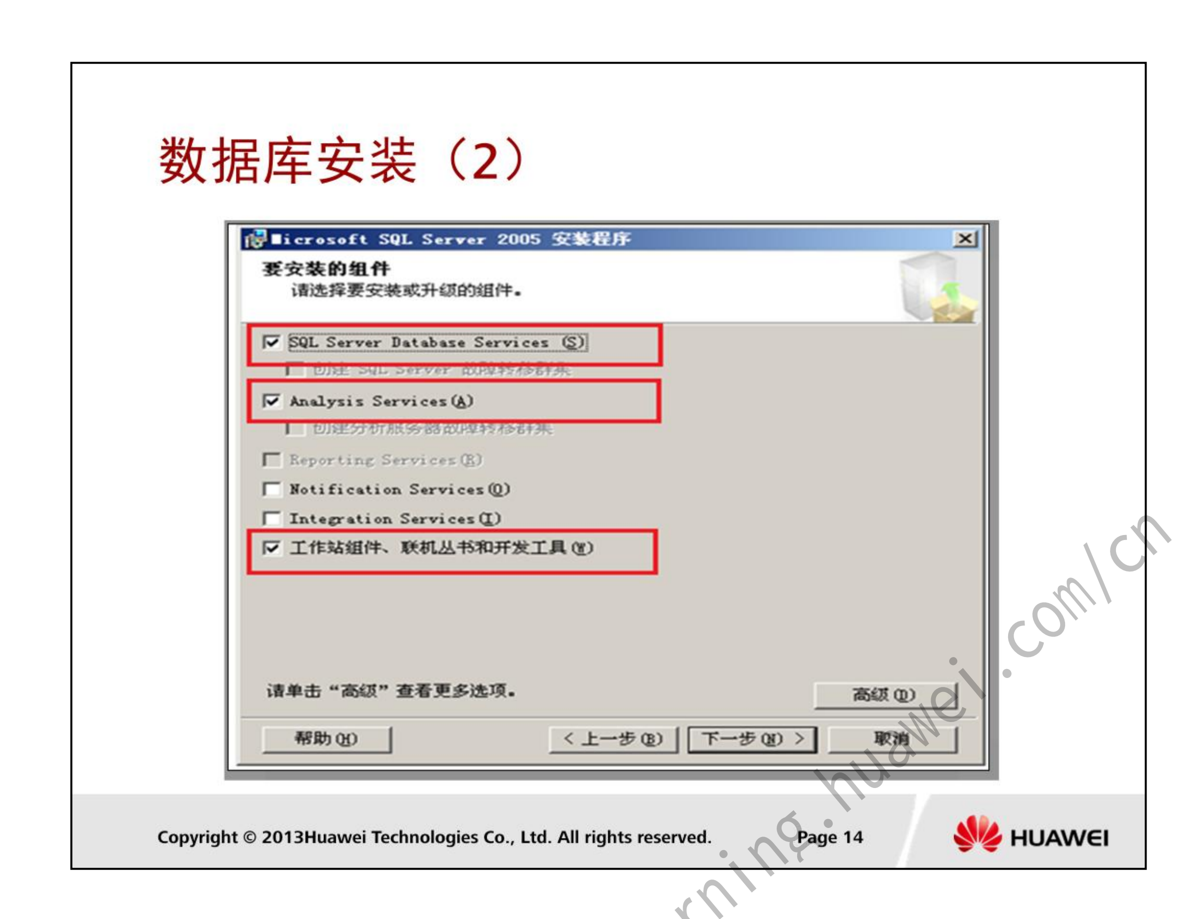
推荐使用Microsoft SQL Server 2005或者Microsoft SQL Server 2008数据库作为产品的数据存储中心，我们将介绍Microsoft SQL Server 2005标准版（32位）的安装过程。Window Server2003的安装在本教材中不做介绍。



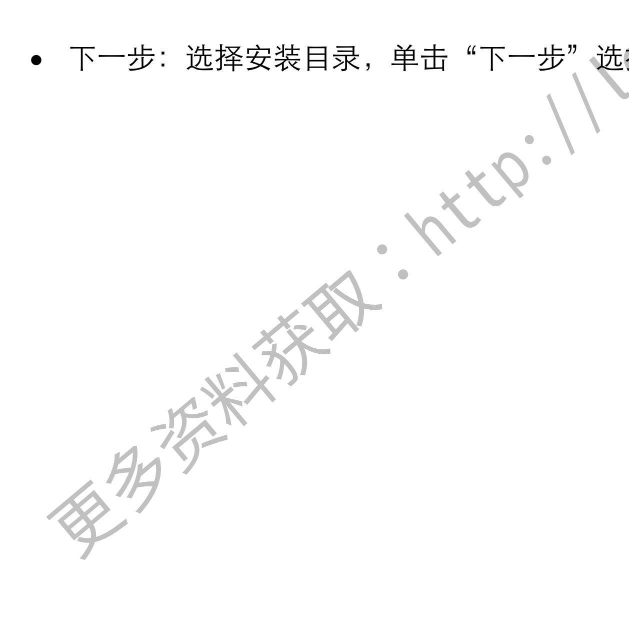
安装Microsoft SQL Server 2005之前需要安装的组件如下：Microsoft .NET Framework 2.0、Microsoft .NET Framework 2.0语言包、Microsoft SQL Server Native Client、Microsoft SQL Server 2005安装程序支持文件，以确保Microsoft SQL Server 2005能够顺利安装并正常运行.

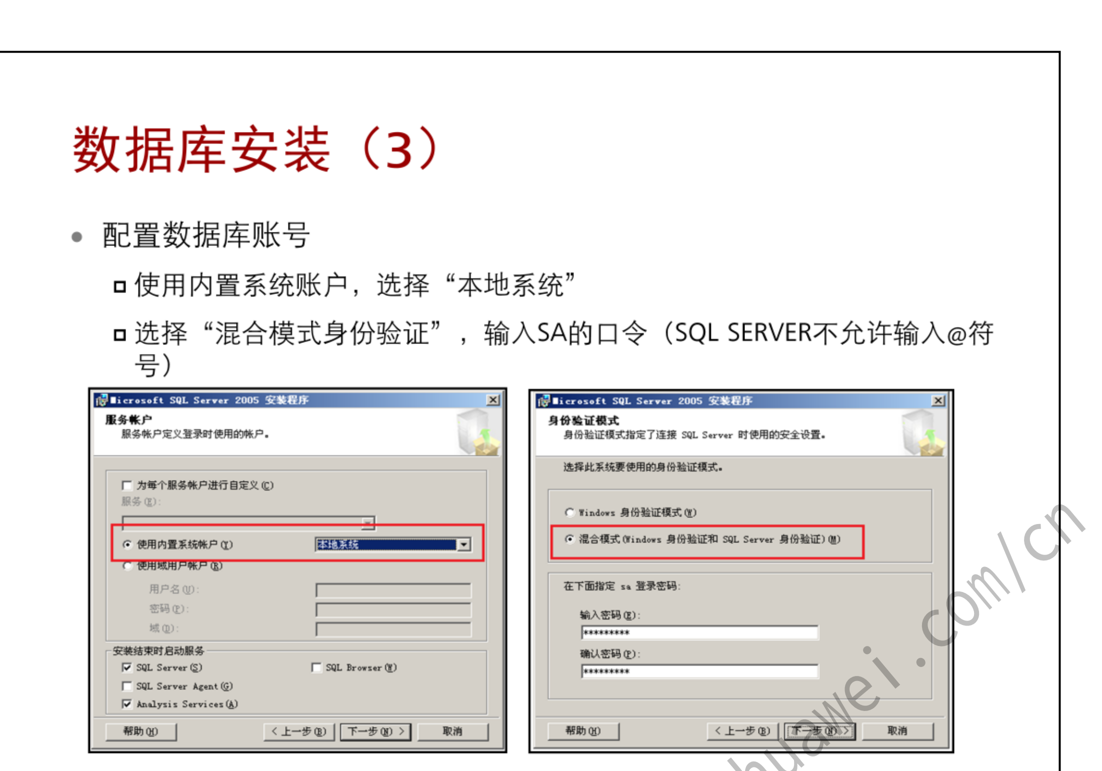


- 下一步：对话框，要求输入公司名称、用户名称、以及产品密钥，完成以后单击“下一步”

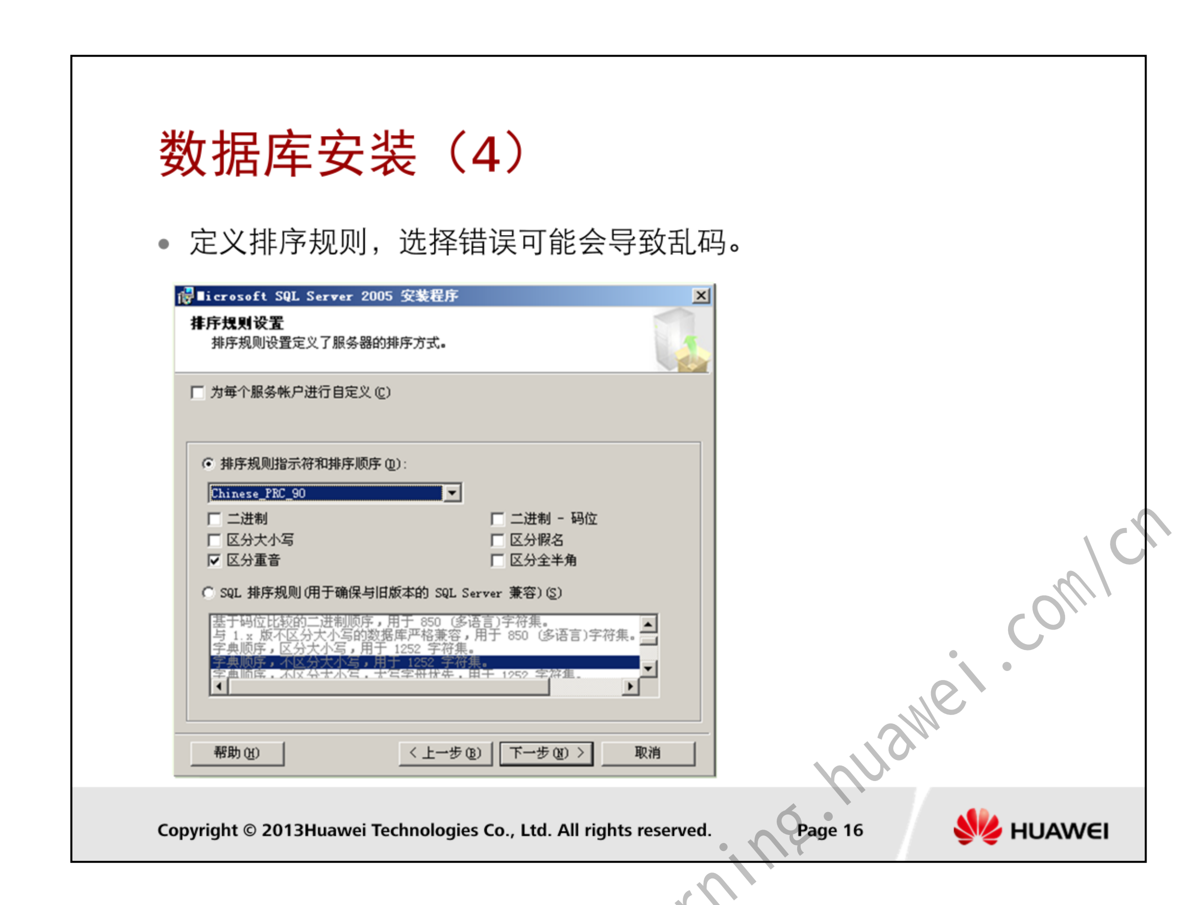


- 下一步：选择安装目录，单击“下一步”选择默认实例

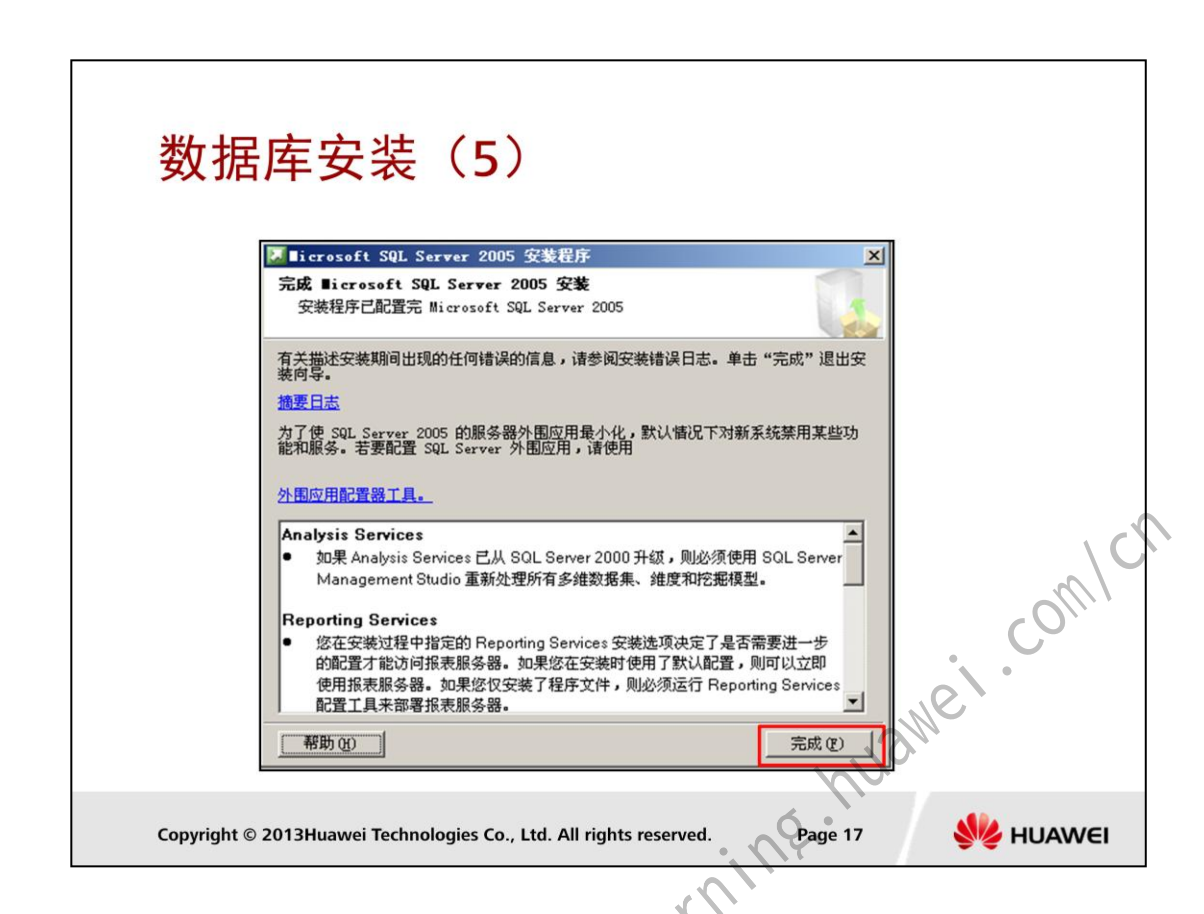




- 需要记住sa密码，在后续安装Policy Center时需要用到。



- 设置数据的排序规则。无论是在中文操作系统还是英文操作系统上安装Microsoft SQL Server 2005，必须将“排序规则指示符和排序顺序”设置为“Chinese_PRC_90”。
- 将“排序规则指示符和排序顺序”设置为“Chinese_PRC_90”的目的在于避免TSM管理器产生乱码，而取消“区分大小写”的目的在于避免因字段大小写导致TSM管理器的报表无法正常显示
- 单击下一步，直至完成安装。



安装完成后可验证安装是否成功，验证方法在胶片中不多做介绍，可查看实验手册。



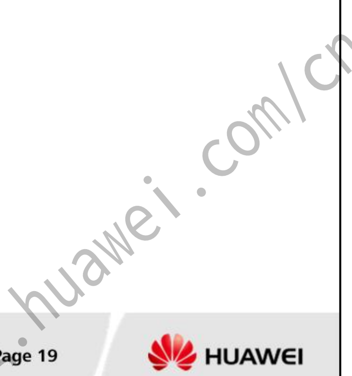


本节主要介绍终端安全系统的安装。

安装Policy Center（1）

- 启动安装
  - 使用Administrator登录操作系统
  - 关闭所有正在运行程序
  - 从发货光碟中找到Policy Center.exe，运行Policy Center.exe

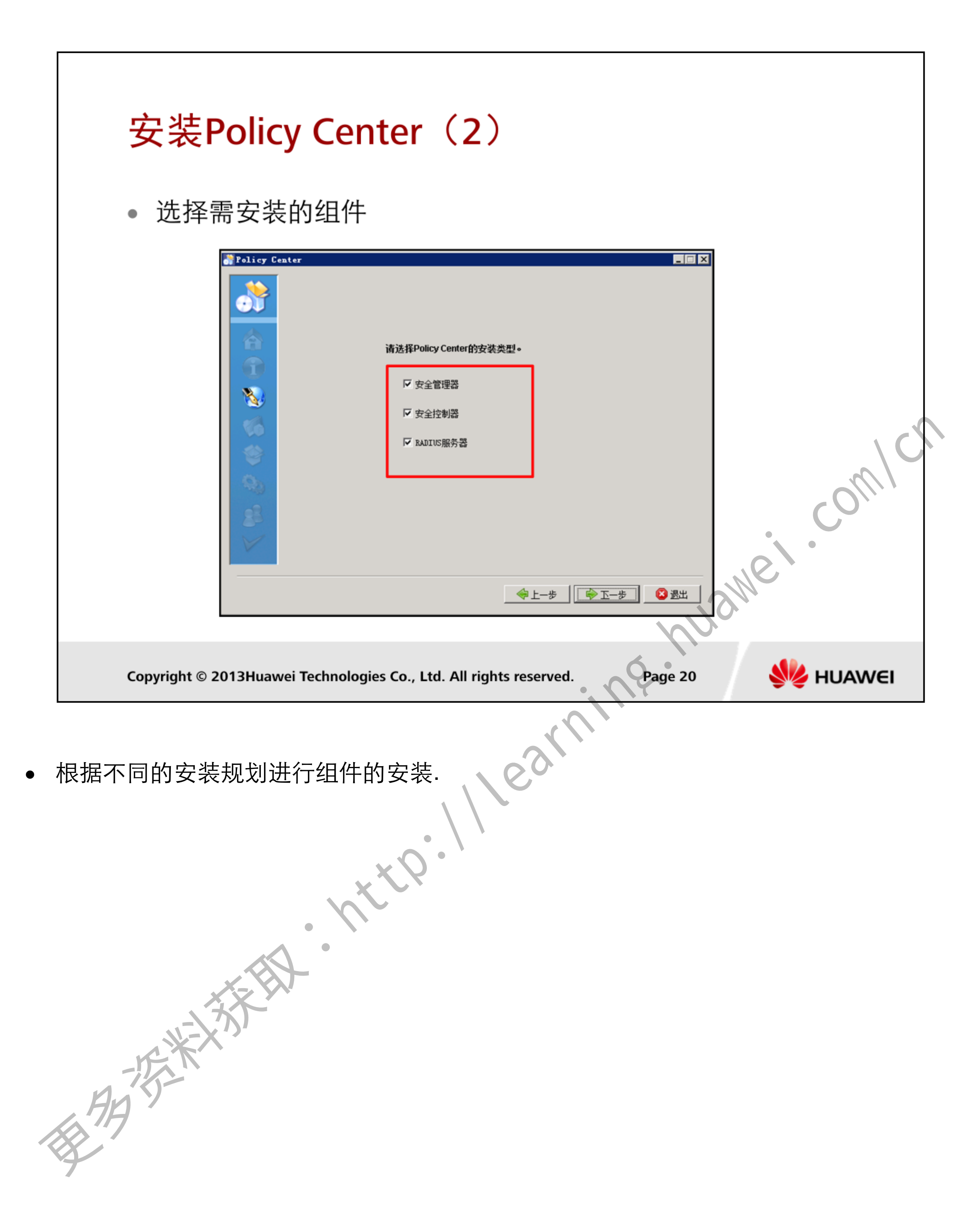




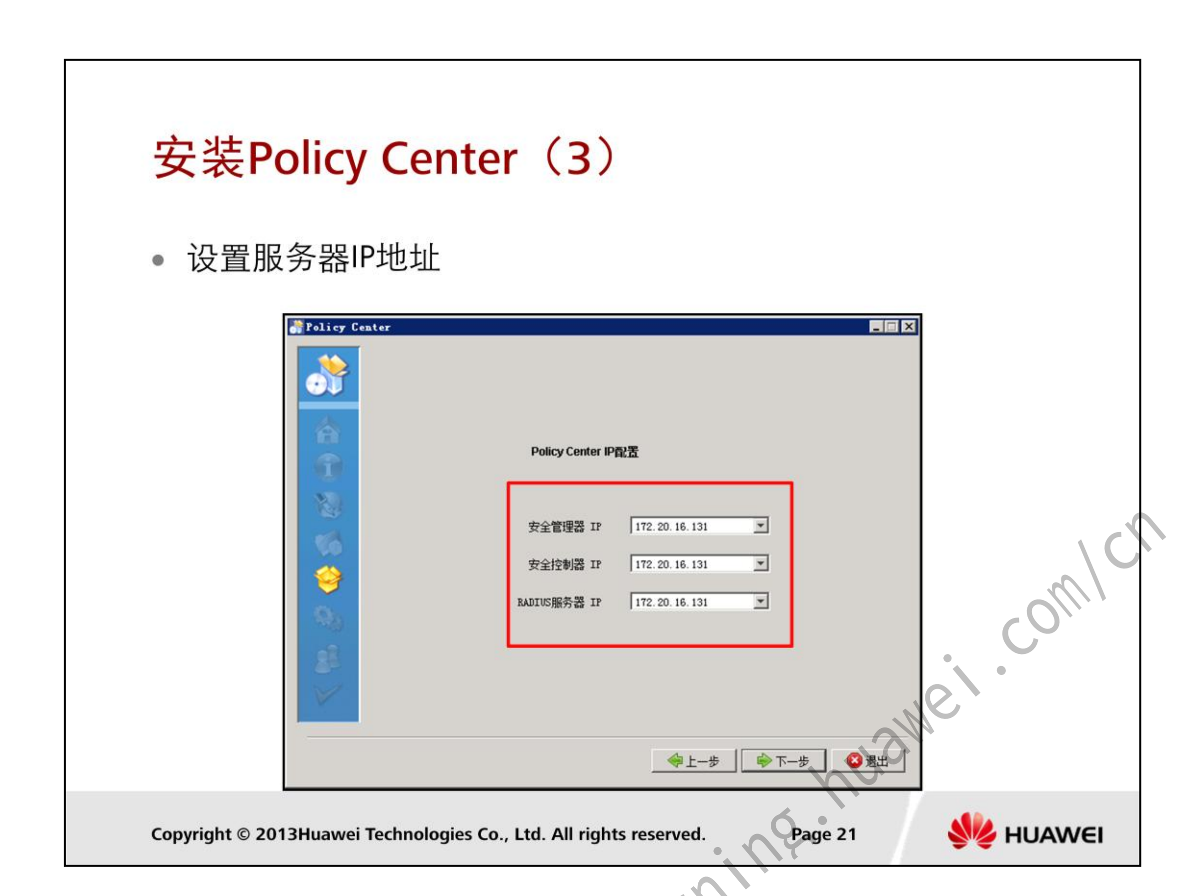
HUAWEI

选择安装语言选择语言请慎重，这里的选择决定了整个产品部署完成后的语言类型。

- 策略管理中心与eSight融合安装，当策略管理中心和eSight同机部署时基本要求如下：
  - 操作系统：Microsoft Windows Server 2008 R2标准简体中文或英文版本，64位，带SP1补丁
  - 数据库：Microsoft SQL Server 2008 R2标准简体中文版或英文版，64位，带SP2补丁



- 根据不同的安装规划进行组件的安装.



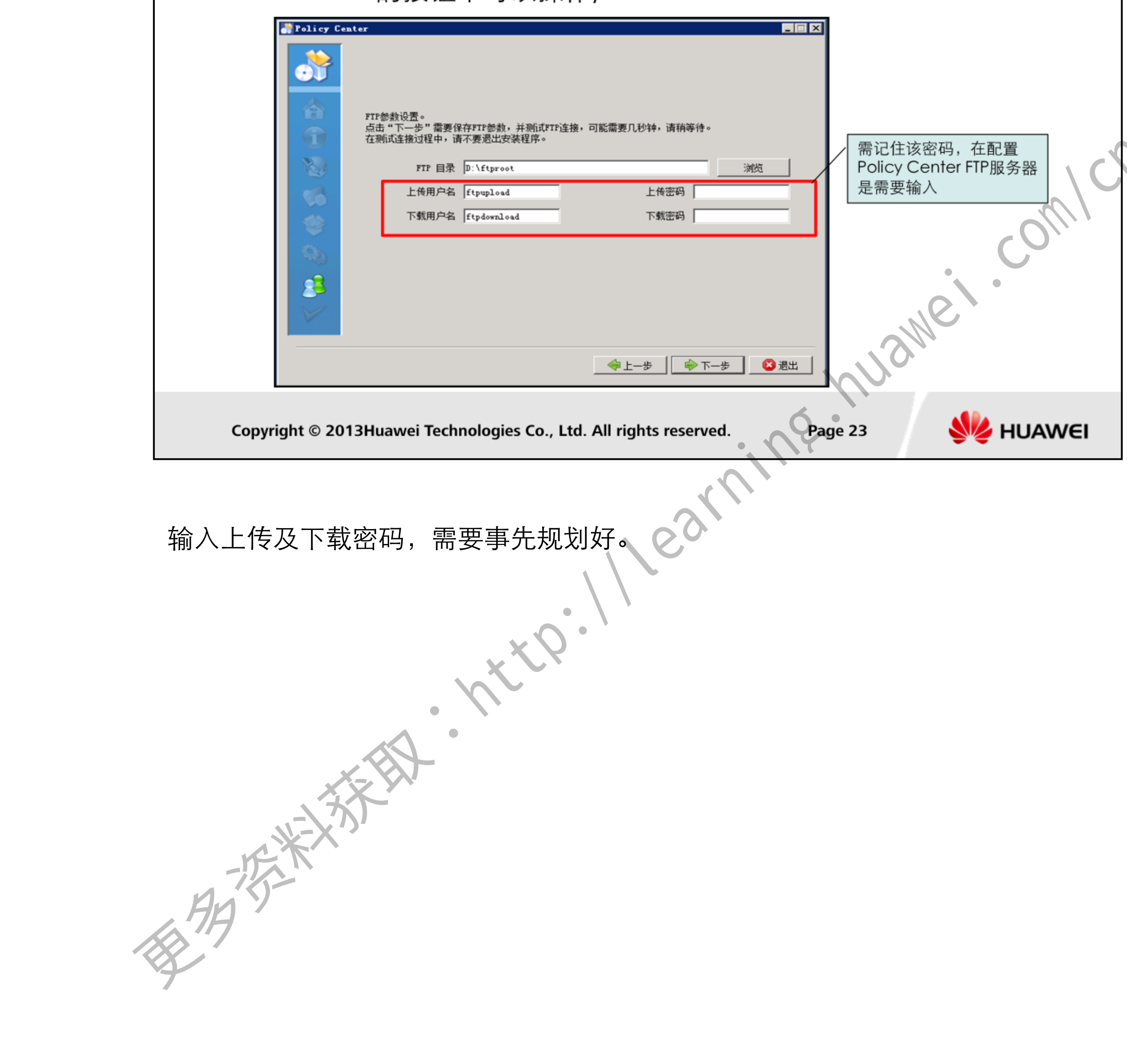
当管理器和控制器安装在同一台硬件服务器时，管理器和控制器使用相同的IP地址。如果安装管理器和控制器的硬件服务器具有多块网卡，请在下拉列表中选择安装管理器和控制器所使用的网卡。



- 配置数据库参数
  - 输入数据库相关参数，测试数据库连接；
  - 测试连接成功后再初始化数据库
  - 推荐最小内存为1024MB，最大内存4098MB



此处sa密码需与数据库的sa密码相同。



输入上传及下载密码，需要事先规划好。

安装Policy Center（6）

- 配置FTP，设置FTP用户名和口令，在“上传密码”和“重复密码”中输入上传用户名对应的密码，推荐的密码长度为8byte～12byte，并且密码不能包含“@”，高级设置默认。



HUAWEI

高级参数是指影响Policy Center服务器运行性能的参数。安装程序默认设置了FTP服务器的高级参数，建议保持默认值。

安装Policy Center（7）

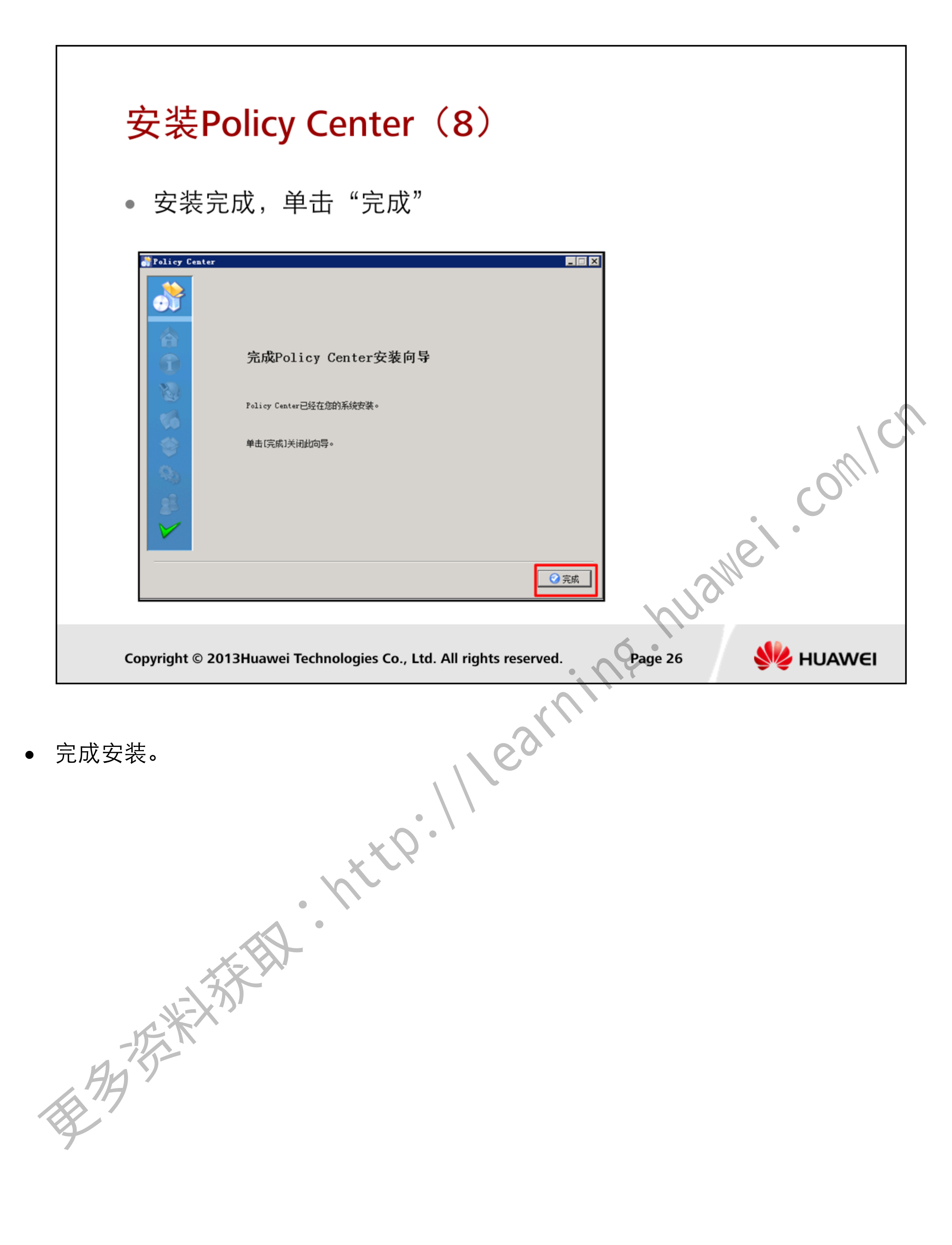
- 保持默认值，单击“下一步”，开始安装管理器和控制器，如下图正在安装管理器和控制器

Policy Center

包安装过程：
C:\Program Files (x86)\Policy Center\jdk\jre\lib\rt.jar
Policy Center安装公共库
进度
1 / 7

上一步 下一步 退出




安装Policy Center（8）
安装完成，单击“完成”
Policy Center
完成Policy Center安装向导
Policy Center已经在您的系统安装。
单击[完成]关闭此向导。
完成
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 26
HUAWEI

- 完成安装。



目录

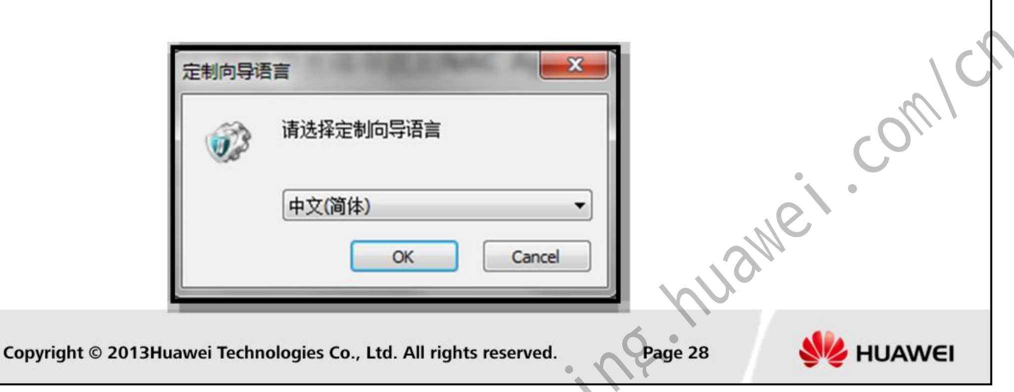


本节主要介绍终端代理定制。



NAC Agent代理定制（1）

- NAC Agent代理定制，即定制终端NAC Agent安装向导，完成定制后得倒NAC Agent.exe，终端双击该程序可安装Agent。
  - 从发货光碟中找到NAC Agent Setup.exe并运行。
  - 选择安装语言。



HUAWEI

定制NAC Agent代理安装程序，为管理员根据网络环境和部署要求生成代理安装程序提供指导。



选择定制Agent安装程序。



- 注意配置控制器地址，完成定制后Agent默认连接地址为1.1.1.2控制器进行认证。



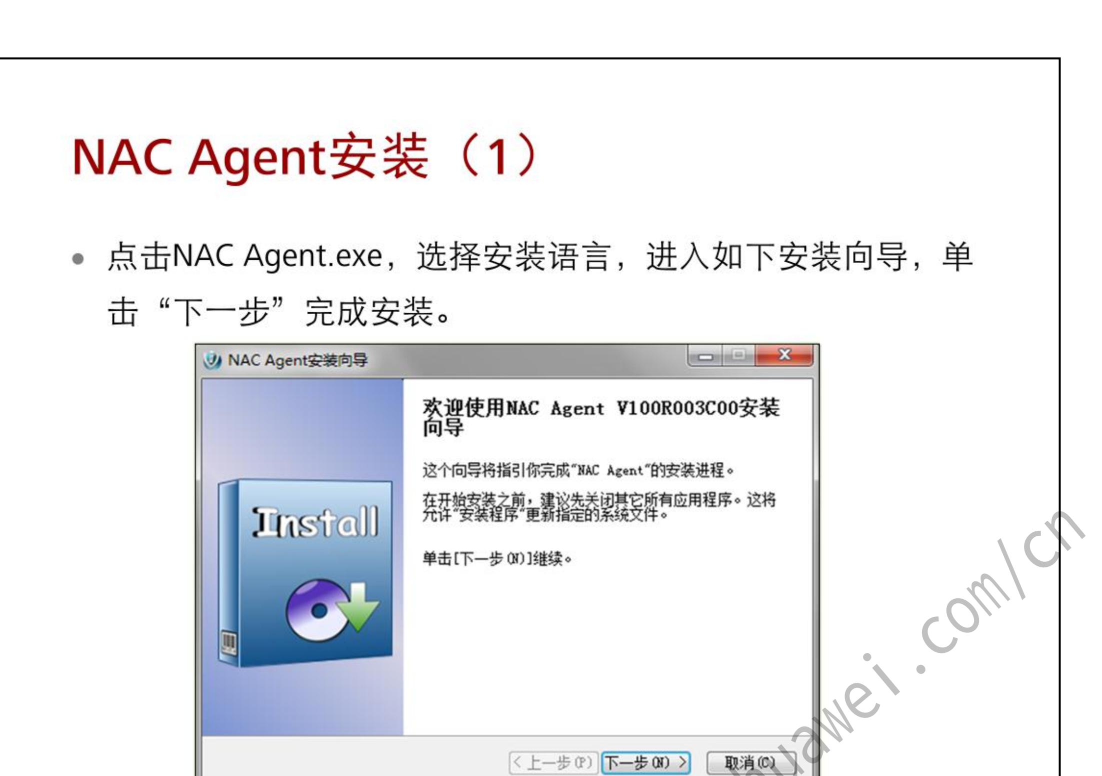
选择是否使用支持802.1x协议的交换机作为硬件安全接入控制网关。在右侧的单元格中的是或否右侧的括号打勾，并根据所使用的交换机类型选择对应的交换机。



- 802.1X协议类型：
  - 使用V1版本的802.1x协议
  - 使用V2版本的802.1x协议
  - 使用HUAWEI Quidway S3528交换机作为硬件安全接入控制网关
- 如果硬件安全接入网关采用支持802.1x协议的交换机，请根据上述三种类型对所有的交换机进行分类，并在交换机贴上分类标签：
  - HUAWEI Quidway S3526交换机
  - 支持802.1x协议V2版本的交换机
  - 支持802.1x协议V1版本的交换机



- 生成NAC Agent代理软件，以上都是在Windows操作系统完成和运行的Agent，NAC Agent也可以安装在linux操作系统，完成检查类策略和监控类策略，但与Windows支持的种类不同。



- NAC Agent.exe默认存放路径是C:\NAC Agent，需注意，NAC Agent的安装是在终端主机上完成的。



NAC Agent安装（2）

- 单击“完成”完成NAC Agent的安装。





目录



- 本节主要介绍终端安全系统License文件管理。

License管理

- License文件用于控制终端安全管理业务。License文件需要向厂家申请，如果没有License文件，则无法使用终端安全系统提供的以下几种业务功能：
  - 接入控制功能
  - 安全管理功能
  - USB管理功能
  - 访客管理功能



HUAWEI

- License文件控制以下功能及使用该功能的用户数。
  - 接入控制功能，包括“接入控制策略”菜单和“用户与终端”菜单的“设备管理”子菜单。
  - 安全管理功能，包括“安全规则管理”、“补丁管理”、“软件分发”和“资产管理”菜单。
  - USB管理功能，包括“USB管理”和“安全规则管理”菜单。
  - 访客管理功能，即“用户与终端”菜单的“访客管理”子菜单。



- 管理器获取License的方式不同，则需要采集的ESN对象也会有所不同：
  - 如果管理器的License由管理中心的管理员统一分配，则只需获取管理中心的ESN。
  - 其他情况由管理器的管理员单独申请并上传License，此时需要获取管理器的ESN。
- 由于ESN与服务器的硬件部件关系非常紧密，在获取ESN后请不要随意更换服务器的硬件部件，否则会导致License无法正常使用。
- 在服务器的硬件部件出现故障后，由于更换部件导致License无法继续使用时，请重新获取ESN，联系并向华为技术工程师反馈ESN和LAC，以便重新申请License。



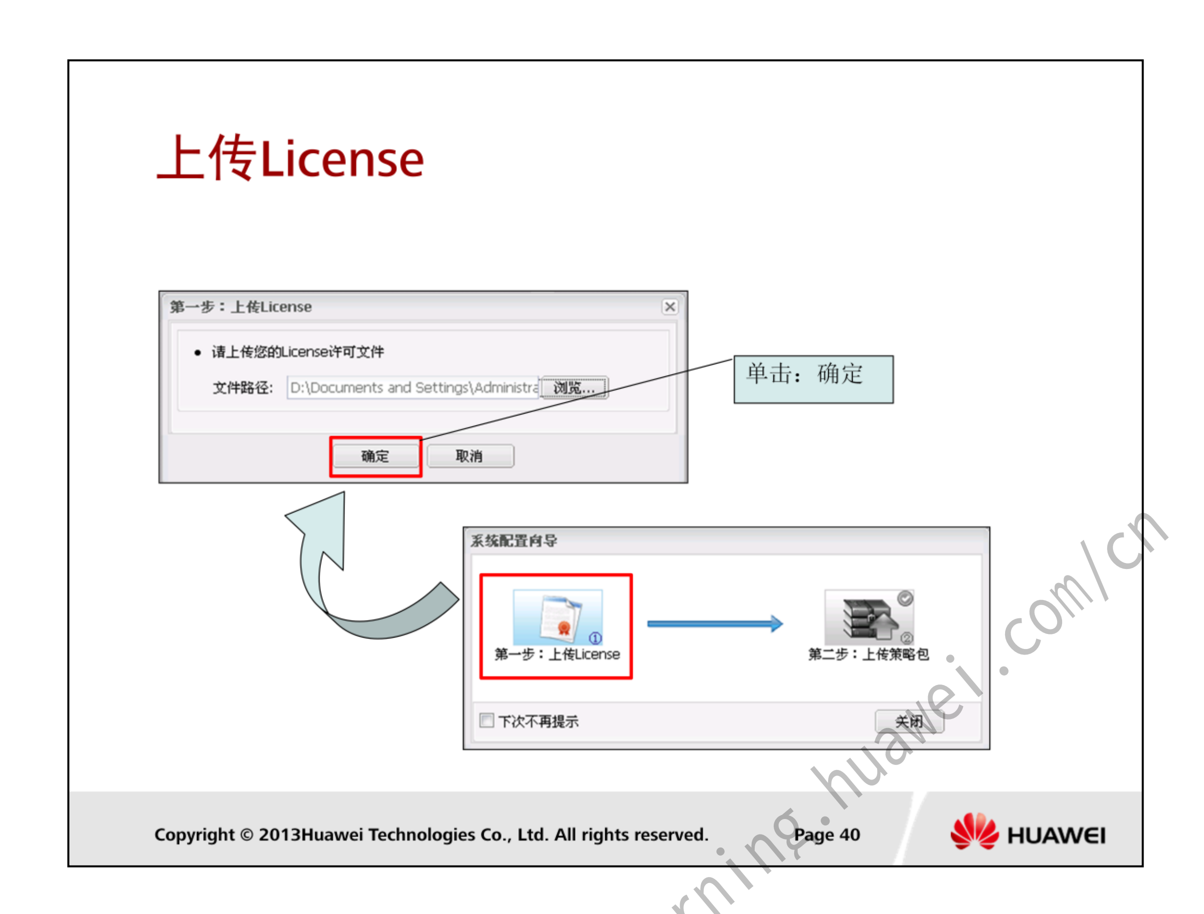
- 在IE浏览器地址栏输入http://"Policy center Server IP":8080

  初始账号：admin 密码：Admin@123



HUAWEI

- 对IE浏览器版本及设置也有要求，具体操作可参照产品手册。



- 管理器的License为 “.DAT”格式的文件。当管理员申请并收到新的License文件后，通过上传License文件实现开放业务权限、增加终端用户并发连接数的目的。



目录



- 本节主要介绍终端安全系统服务器配置。

SC配置

- 配置路径：系统配置>SC配置，单击“增加”设置控制器的名称及IP地址。
- 安全管理器不会校验所输入的IP地址是否存在或安全控制器是否存活。管理员在为归属地分配安全控制器时确保安全控制器可用即可。

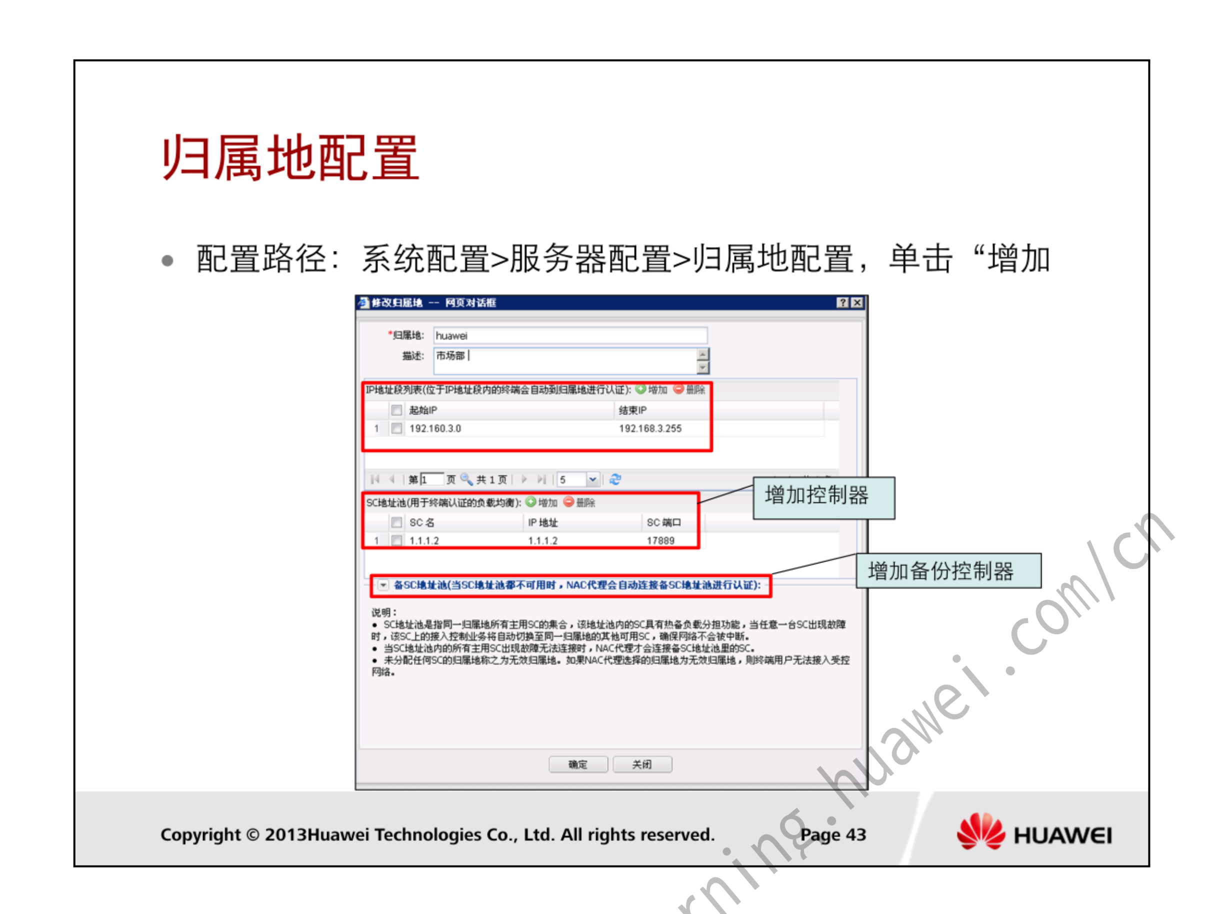


控制器支持将违规数据实时上报或缓存上报到数据库。缓存上报方式适用于终端安全系统部署采用分布式组网的场合。通过设置在业务空闲期上报违规数据，能够避免违规数据的上报占用大量网络带宽，影响业务运行。

缓存上报方式需要指定违规数据的上报时间段。违规数据以缓存方式上报时，控制器将以一天为周期向数据库上报违规数据。 当天的上报时间到来之前，已经缓存的违规数据通过即刻上报能够立即上报到数据库，供管理员查看。在即刻上报过程中，管理员能够手动停止上报。即刻上报未上报完的违规数据将在上报时间到来之后再上报到数据库。

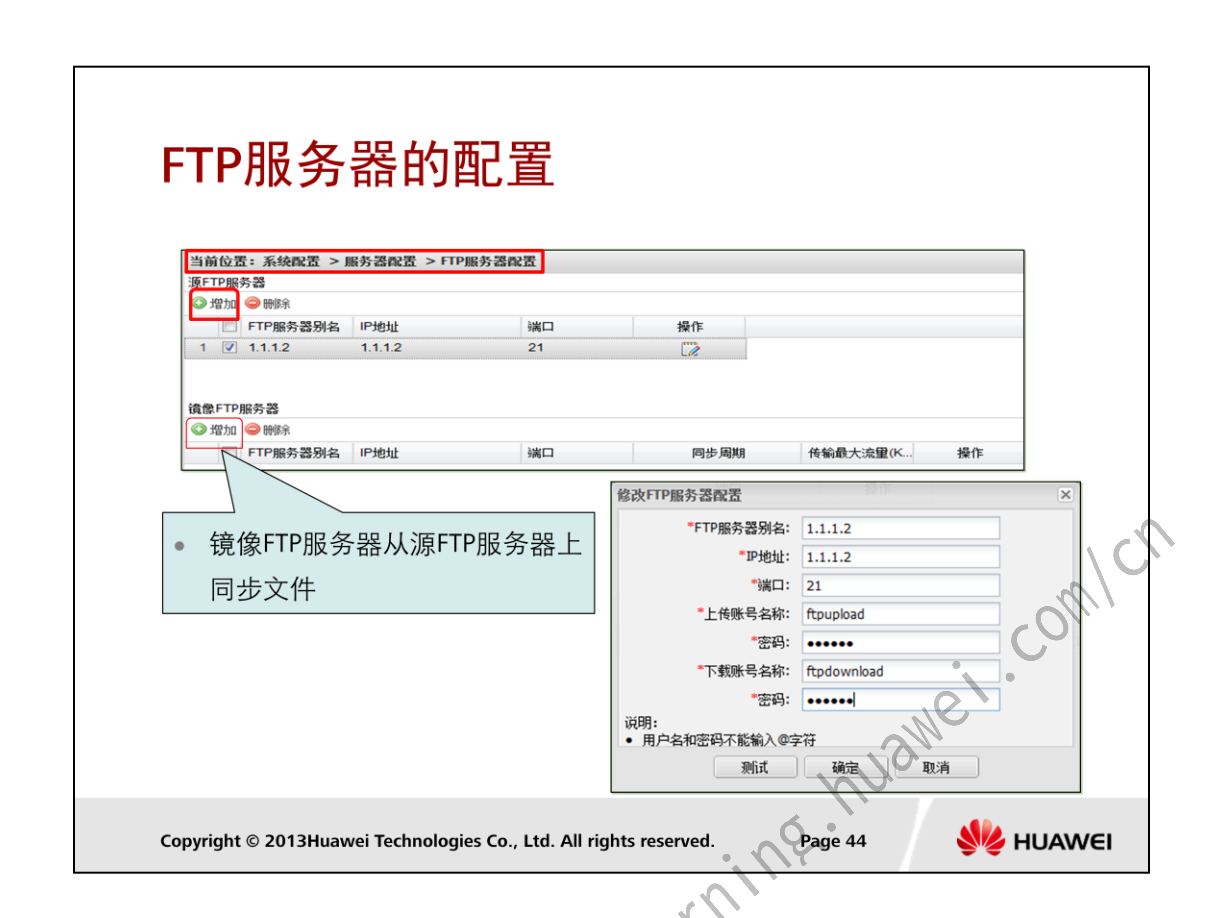
当天的上报时间结束后，控制器将立即停止上报违规数据。对于上报时间结束而违规数据没有上报完成的情况，管理员通过设置Server Monitor的过滤告警项目，能够监控违规信息是否上报完成，以便确认是否需要调整缓存上报的“持续时间”。如果 Server Monitor多次产生缓存上报未完成的告警信息，建议管理员延长缓存上报的“持续时间”。

Server Monitor是Policy center的运维工具在下面的胶片将会介绍。



增加归属地，以便管理器将归属于同一个归属地的所有主用控制器和备用控制器加入地址池，确保地址池的所有控制器共同分担负荷，在其中的控制器出现故障时确保网络连接不会被中断

现网部署多台控制器，这些控制器构成了终端认证的地址池。在认证时，客户端随机地从地址池中选择一台控制器进行连接，从而达到对控制器进行负载分担的目的。当地址池中的所有控制器出现故障时，通过提供备用控制器，确保客户端能够连接备用控制器完成认证，提高了服务器的可靠性



还可增加源FTP服务器，方便管理员存放安全策略、软件和补丁，同时向终端用户和镜像FTP服务器提供安全策略、软件和补丁的下载服务



- FTP服务器的分配原则如下：
  - 如果安全管理器与安全控制器安装在同一台硬件服务器，则不需要配置备选FTP服务器，只需要配置首选FTP服务器，首选FTP服务器指向安全管理器即可。
  - 如果安全管理器与安全控制器安装在不同的硬件服务器，并且只包含一台安全控制器，则不需要配置备选FTP服务器，只需要配置首选FTP服务器，首选FTP服务器需要指向安全控制器。
  - 如果安全管理器与安全控制器安装在不同的硬件服务器，并且包含多台安全控制器，则需要同时配置首选FTP服务器和备选FTP服务器。首选FTP服务器需要指向与NAC Agent连接带宽最好的安全控制器，备选FTP服务器需要指向其他安全控制器。



目录



- 本节主要介绍终端功能配置。

全局参数

- 终端全局参数是与客户端相关的参数，配置该参数后对所有终端都适用，根据实际需要配置各类全局参数。

当前位置：系统配置 > 终端配置 > 全局参数

配置路径

终端代理自启动和非AD域用户登录设置

终端代理强制自启动设置:	启用	禁用
配置同一账号能在多个终端登录:	启用	禁用
配置非AD域用户启用域账号登录:	启用	禁用
显示ARP页面:	启用	禁用
允许终端查看设备状态:	启用	禁用
拔出USBKey后客户端是否自动注销（仅支持终端代理）:	启用	禁用

确定

配置代理终端认证类型

配置子网快速下载参数

配置违规上报周期参数

配置下推主页URL

配置定制的终端的显示标题和显示图标

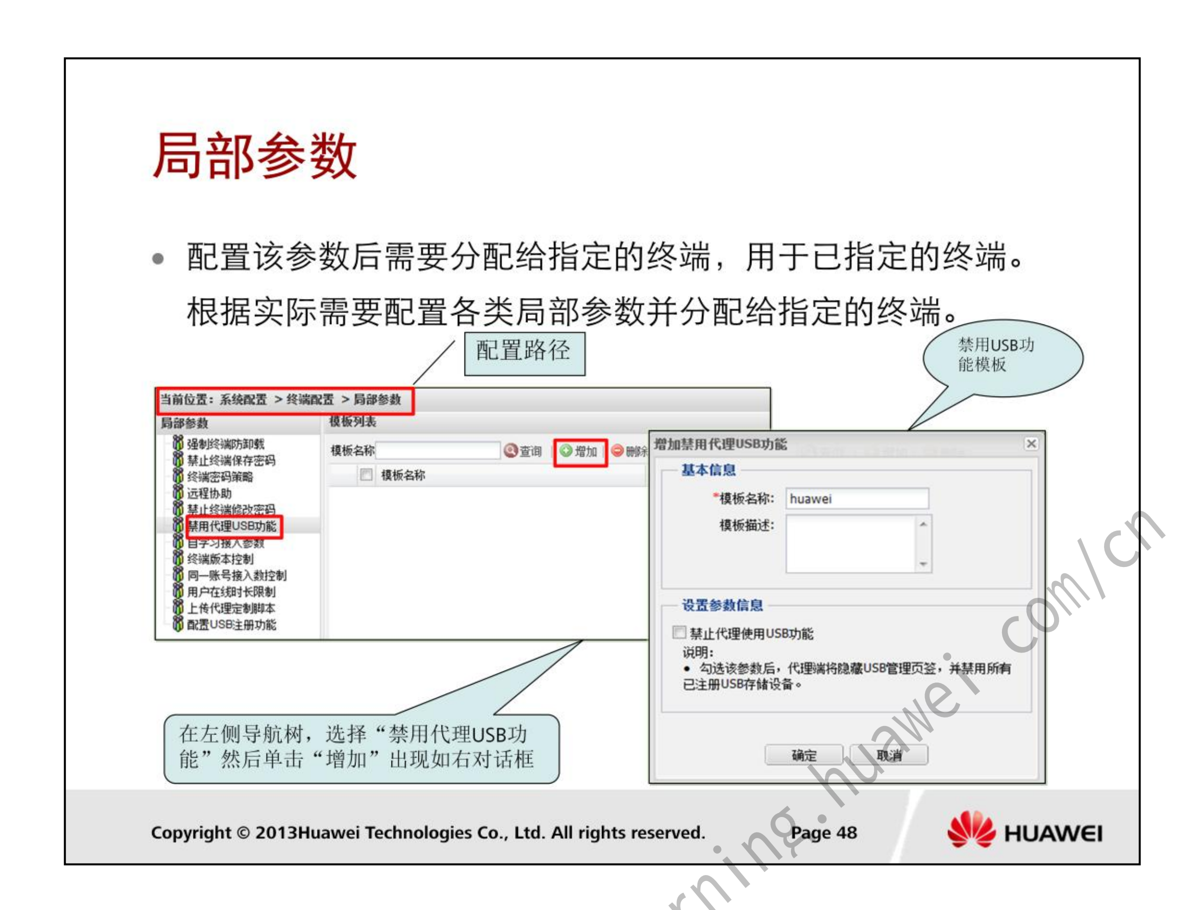
配置远程采集日志密码

网络导航

HUAWEI

设置终端参数，功能较为丰富，通过在管理器的设置使终端代理具备或不具备某些功能。

- 主要参数：
  - 终端代理自动和非AD域用户登录设置。
  - 终端认证类型
  - 违规上报周期
  - 下推主页URL
  - 802.1X认证
  - 网络导航
  - ………



局部参数是与NAC Agent的配置相关的参数，只在下发了局部参数模板的终端生效，如果不同的模板分配给部门、账号、终端IP地址范围，则优先级最高者所分配到的模板将会生效。部门、账号、终端IP地址范围的优先级关系为：账号 > 终端IP地址范围 > 部门。

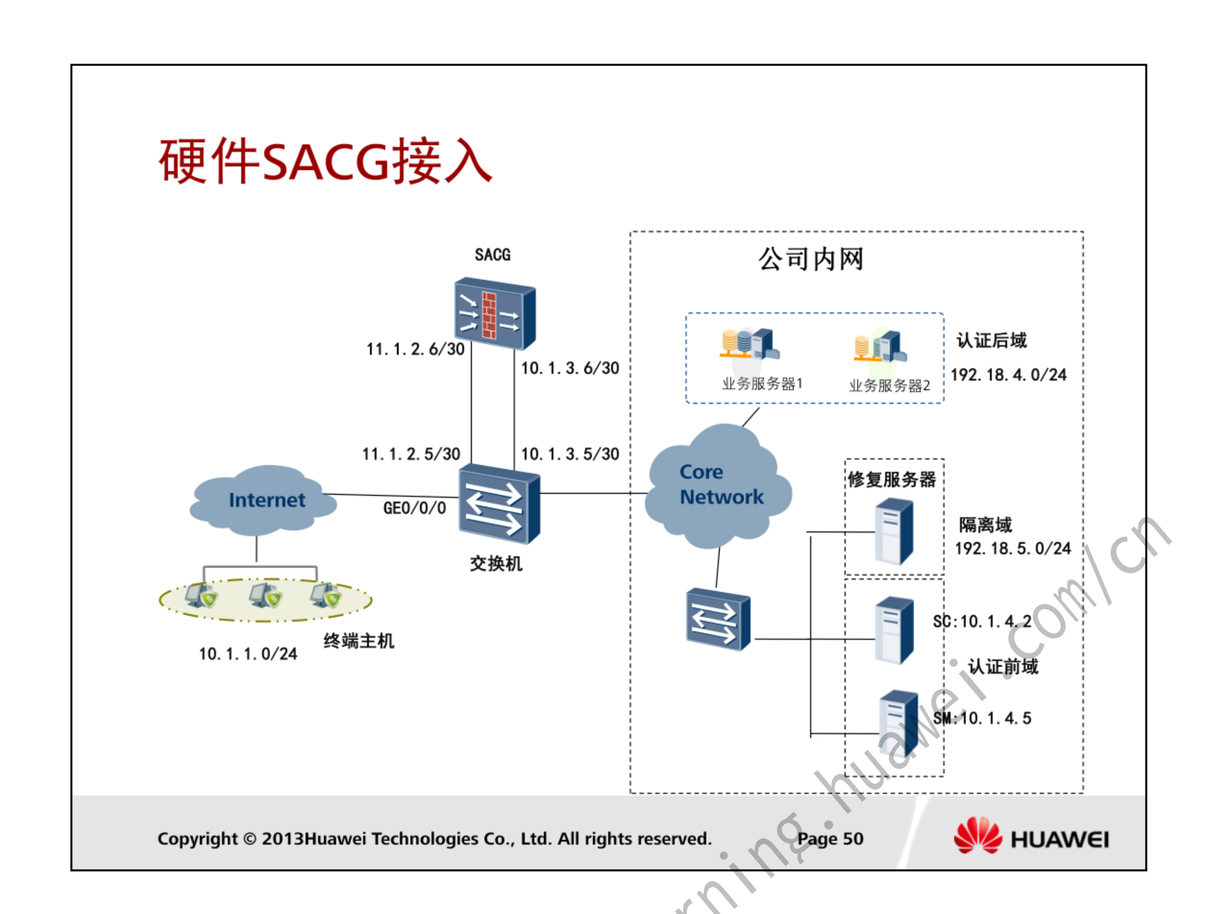
- 终端局部参数：
  - 强制终端防卸载：禁止终端用户随意卸载NAC Agent，卸载时要求输入管理员提供的卸载密码。
  - 禁止终端保存密码：NAC Agent的认证界面不展示“保存密码”复选框，终端用户以NAC Agent方式认证时不能保存密码。
  - 远程协助：在NAC Agent界面显示远程协助的配置界面，终端用户能够修改是否允许管理员远程控制或查看终端主机的桌面。
  - 禁止终端修改密码：终端用户在NAC Agent使用普通账号认证通过后，禁止该用户修改账号的密码。
  - 禁止终端USB功能：终端用户在NAC Agent通过认证后，禁止该用户使用注册的USB移动存储设备，这部分终端不占用USB管理功能的License。



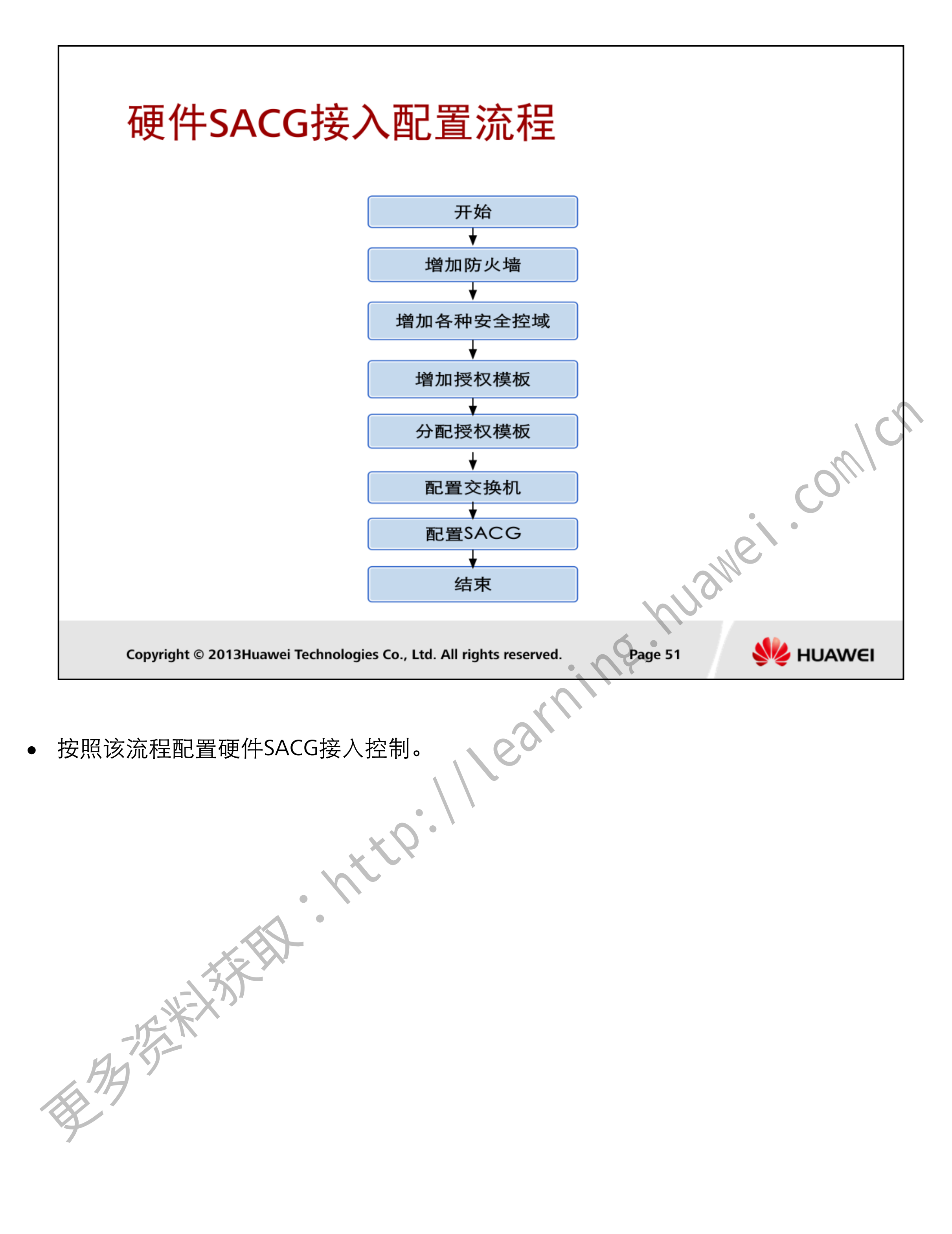
目录



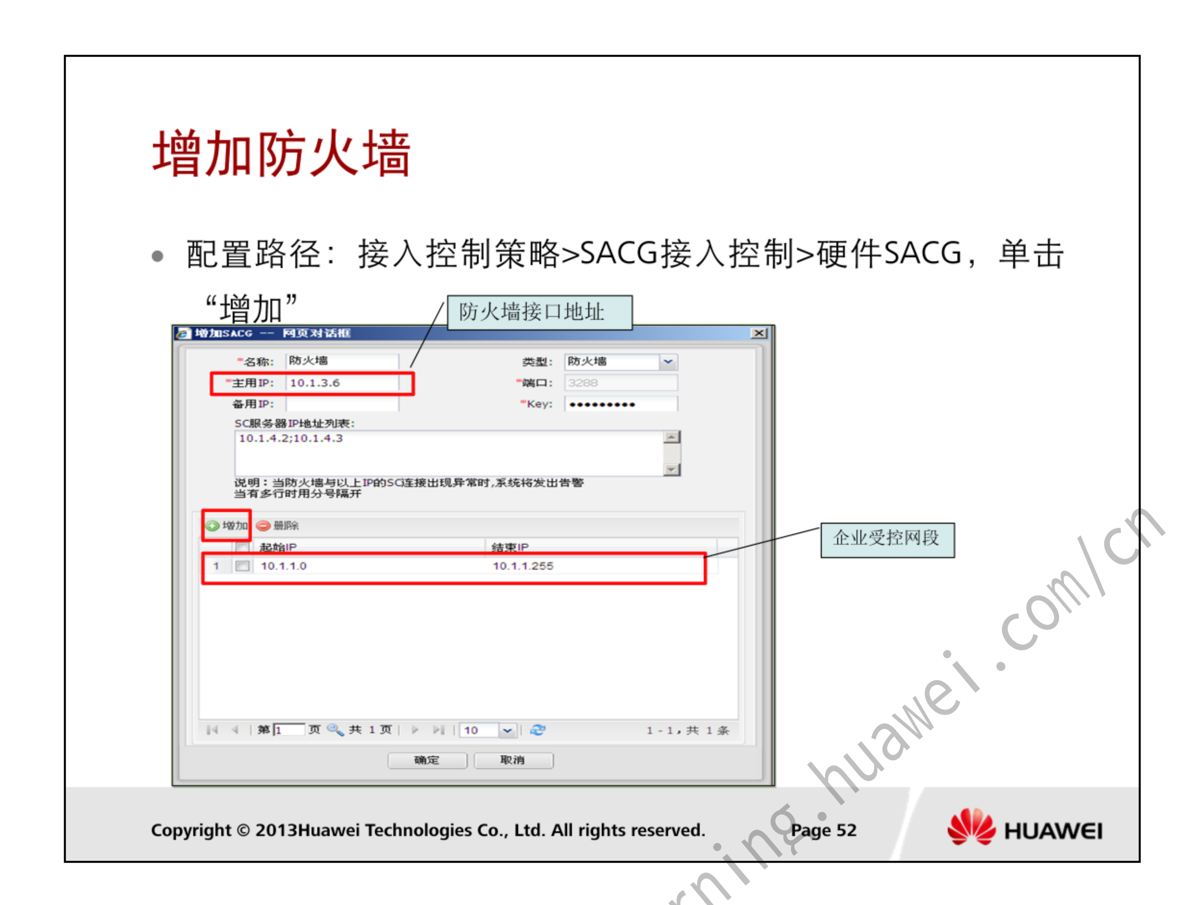
- 本节主要介绍终端安全系统的部署



硬件SACG典型组网拓扑，旁挂方式，IP规划如图中所示，其中SACG为USG5300，版本为V3R1，策略中心可与多种型号及版本的防火墙联动，具体型号及版本的对应关系可查看产品文档。



- 按照该流程配置硬件SACG接入控制。



- 主要参数说明：
  - 名称：设置硬件安全接入控制网关的名称，该名称不能与已存在的硬件安全接入控制网关名称重复。最大长度为100byte。
  - 类型：选择硬件安全接入控制网关的类型。这里使用防火墙来控制终端用户接入网络，请选择“防火墙”。
  - 主用IP：输入防火墙设备连接到控制器的接口的IP地址。
  - 备用IP：如果现网提供备用防火墙设备，输入备用设备连接到控制器的接口的IP地址。
  - Key：输入防火墙设备的认证密码，必须与防火墙设备配置的共享密钥一致。
  - SC服务器IP地址列表：输入连接异常需要产生告警的控制器的IP地址。当防火墙与“SC服务器IP地址列表”中的控制器连接异常时，管理器将发出告警。当有多个IP地址时，请用半角分号分隔开。

增加前域

- 配置路径：接入控制策略>SACG接入控制>硬件SACG，单击"前域"

增加前域

*IP地址：10.1.4.2

*掩码长度（位）：32

描述：TSM控制器。

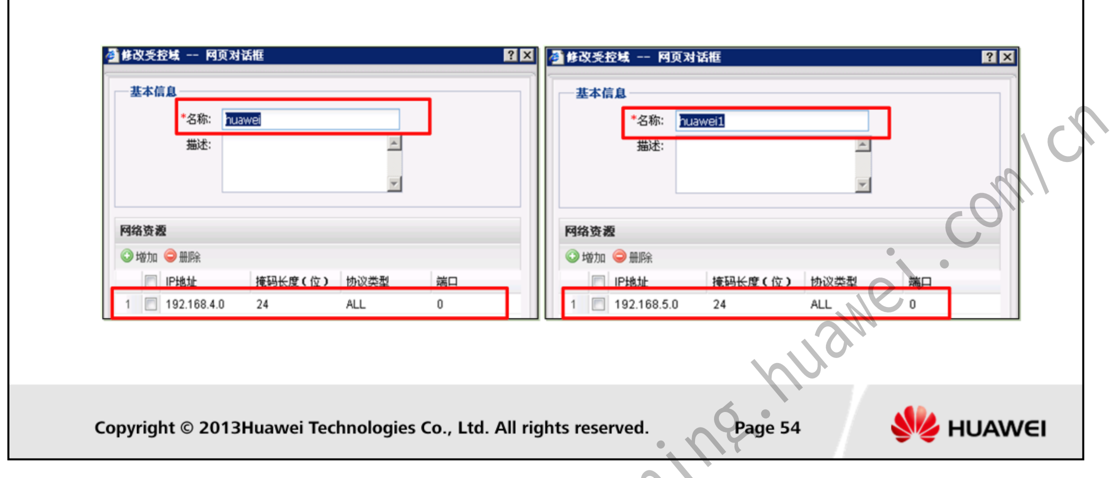
确定　取消

HUAWEI

- 硬件安全接入控制网关只允许配置1个认证前域，该认证前域适用于所有的终端用户。
- 认证前域最多支持增加500条IP地址段记录，所有的IP地址段作为认证前域所包括的网络资源。
- 请将以下网络资源部署在认证前域：允许终端用户在通过身份认证之前访问的公共网络资源（如DNS服务器、外部认证源、控制器、管理器等）。
- 如果在"SC配置管理"页面中管理员已经列出所有的控制器，则所有的控制器（包括不属于该归属地的控制器）均会自动加入认证前域，否则，需要管理员手工将所有的控制器加入认证前域。



- 配置路径：接入控制策略>SACG接入控制>硬件SACG，单击“受控域”
- 创建两个受控域，分别对应于隔离域和认证后域网段



- 硬件安全接入控制网关允许配置多个受控域。
- 将终端用户在认证后才能访问的所有网络资源添加到受控域中，根据终端用户的权限不同，不同的受控域配置为隔离域和认证后域。例如，对于部门A，将受控域1配置为部门A的隔离域，将受控域2配置为部门A的认证后域

增加隔离域

- 配置路径：接入控制策略>SACG接入控制>硬件SACG，单击“隔离域”选择名称为“huawei_隔离”的受控域

HUAWEI

- 能够帮助终端用户消除违规信息的相关资源（如补丁服务器、防病毒服务器等）部署在本区域，硬件安全接入控制网关允许配置多个隔离域。
- 选择“禁止访问列表中的受控域资源，允许访问其它。”：禁止接入认证后域的终端用户访问“受控域资源”列出的受控域中的网络资源，但允许终端用户访问“受控域资源”未列出的受控域中的网络资源。
- 该选项适用于禁止终端用户访问的网络资源非常容易全部列举出来，但允许终端用户访问的网络资源较多或者不容易全部列举出来的情况。
- 在认证后域中，除非明确禁止终端用户访问的网络资源，其他未涉及的网络资源在缺省情况下是允许终端用户访问的。要实现终端用户通过认证后能够访问Internet的功能（将Internet作为管理器的认证后域），必须使用“禁止访问列表中的受控域资源，允许访问其它。”模式



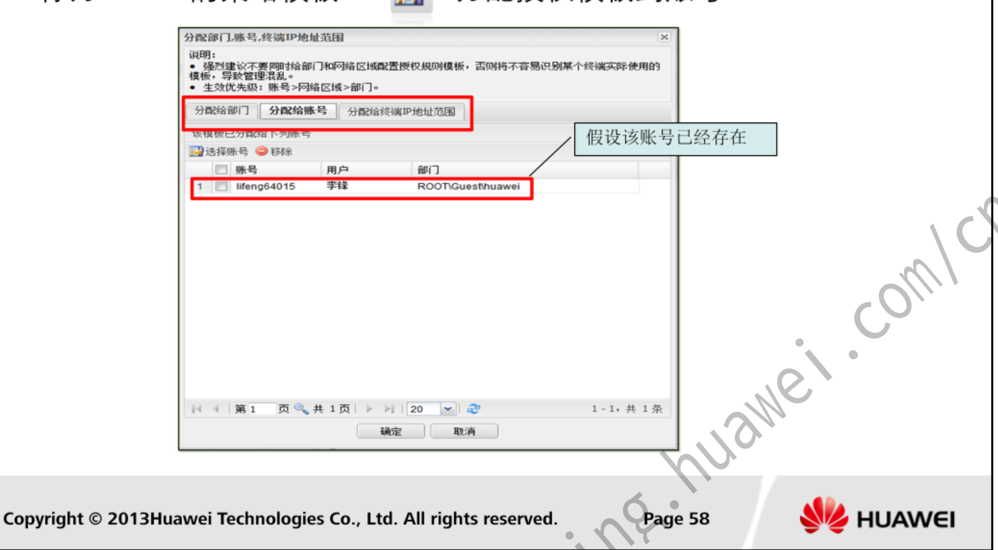
- 需要受控访问的网络资源（如ERP系统、财务系统、数据库系统）部署在本区域，硬件安全接入控制网关允许配置多个认证后域。



- 增加硬件安全接入控制网关的授权规则模板，以便将所创建的隔离域和认证后域分配给终端主机，确保终端主机在认证通过后能访问相应的网络资源。
- 在不同时间段和不同认证状态下访问相应的网络资源，以便验证硬件安全接入控制网关按时间段接入控制配置成功。
- 根据终端用户进行认证的时间，以及认证状态不同，终端用户能够访问的网络资源也不同，具体情况如下：

分配授权规则模板

- 配置路径：接入控制策略>SACG接入控制>授权规则模板，单击名称为huawei的策略模板“ ”分配授权模板到账号。



应用隔离域和认证后域到网络区域/账号/部门，当该网络区域所分配到的隔离域和认证后域生效时，通过身份认证但未通过安全认证的终端主机只允许访问隔离域的网络资源，通过安全认证的终端主机允许访问认证后域的网络资源。

如果在设置网络区域的隔离域和认证后域时，设置了部门、账号的隔离域和认证后域，则三者中优先级最高者所分配到的隔离域和认证后域将会生效。部门、账号、网络区域的优先级关系为：账号 > 网络区域 > 部门。

当同时为部门和网络区域分配隔离域和认证后域时，管理员要判定某个员工对应的隔离域和认证后域，不仅要考虑员工在哪个部门，还要考虑该员工在哪个网络区域的终端主机上进行认证。当员工在不同网络区域认证时，各个网络区域配置的隔离域和认证后域不一样，员工对应的隔离域和认证后域也就不一样。这就增加了管理员管理的复杂度。因此，建议管理员不要同时为部门和网络区域分配隔离域和认证后域。

下发访问控制列表

当前位置：接入控制策略 > SACG接入控制配置 > 硬件SACG

硬件SACG | 前域 | 受控域 | 隔离域 | 后域 | BAS后域

增加 删除 同步硬件SACG 导入 导出

		名称	类型	操作
1		nosacg	不启用	
2		huawei	防火墙	

单击“同步硬件SACG”弹出对话框如右，单击“是”

提示

确定同步硬件SACG?

是 否

HUAWEI

- 操作步骤：
  1. 选择“接入控制策略 > SACG接入控制配置 > 硬件SACG”。
  2. 选择“硬件SACG”页签。
  3. 单击“同步硬件SACG”。
  4. 单击“是”。
  5. 访问控制列表将会立即被下发至硬件安全接入控制网关并且立即生效。

交换机关键配置

- 交换机需要把进入交换机的流量重定向到SACG，由SACG控制数据流的转发，常用有三种配置方法：
  - 接口使用traffic-redirect命令
  - 策略路由
  - 使用流分类、流行为、流策略
- 举例：直接在接口使用traffic-redirect命令：

  [SW-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255

  [SW-GigabitEthernet0/0/0] traffic-redirect inbound acl 2000 ip-nexthop 11.1.2.6



- 基础配置：接口类型、IP地址等，省略
- ACL配置：需要进行准入控制的网段[SW-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
- 重定向配置：
  - 在接口使用traffic-redirect命令：

    [SW-GigabitEthernet0/0/0] traffic-redirect inbound acl 2000 ip-nexthop 11.1.2.6
  - 策略路由：

    [SW]policy-based-route redirect permit node 1

    [SW-policy-based-route-redirect-1]if-match acl 2000

    [SW-policy-based-route-redirect-1]apply ip-address next-hop 11.1.2.6
  - 流分类、流行为、流策略配置：

    [SW]traffic classifier c-redirect

    [SW-classifier-c-redirect]if-match acl 2000

    [SW]traffic behavior b-redirect

    [SW-behavior-b-redirect]redirect ip-nexthop 11.1.2.6

    [SW-trafficpolicy-p-redirect]classifier c-redirect behavior b-redirect
  - 应用到接口
    - 策略路由：[SW-GigabitEthernet0/0/0]ip policy-based-route redirect
    - 流分类、流行为、流策略：[SW-GigabitEthernet0/0/0]traffic-policy p-redirect inbound

SACG关键配置

- SACG一般常用防火墙也可以是BAS设备（华为ME60），如果为防火墙一般使用USG和Eudemon系例防火墙，配置命令基本相同。
- USG系列防火墙配置举例：

[USG5000] **right-manager server-group**

[USG5000-rightm] **default acl 3099**

[USG5000-rightm] **server ip 10.1.4.2 port 3288 shared-key TSM_Security**

[USG5000-rightm] **right-manager server-group enable**

[USG5000] **policy interzone trust untrust outbound**

[USG5000-policy-interzone-trust-untrust-outbound] **apply packet-filter right-manager**



- 当终端用户在未通过身份认证的情况下通过IE浏览器尝试访问认证后域中的Web服务器时，配置USG5000以便实现USG5000自动在终端主机推送Web认证页面的功能，方便终端用户通过Web页面进行身份认证。

  [USG5000] right-manager server-group

  [USG5000-rightm] right-manager authentication url http://10.1.4.2:8080/webauth

- 配置与USG5000连接控制器的最少数量，并启用逃生通道功能

  [USG5000-rightm] right-manager server-group active-minimun 2

  [USG5000-rightm] right-manager status-detect enable

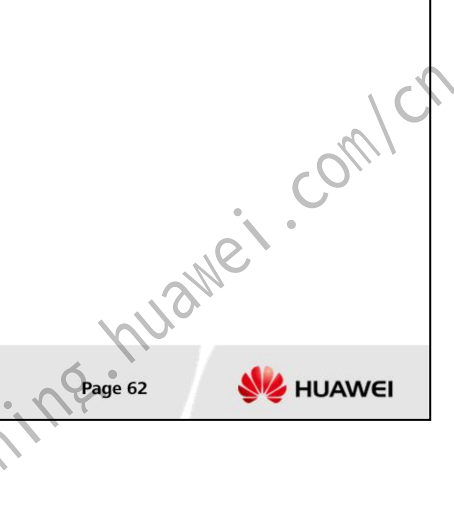
  逃生通道的状态切换描述如下：

  - 当存活的控制器达到或超过2（active-minimun参数右侧的参数值，取值范围为1～8，默认值为1）台时，USG5000将不会开启逃生通道。
  - 当存活的控制器小于2台时，USG5000将会开启逃生通道，允许所有用户终端访问受控网络，避免终端用户因控制器出现故障而无法访问网络。

- 不同版本的防火墙在策略管理中心联动配置命令有所差异，但基本类似，实际配置时请参考相应产品文档。
- 注意：需配置返回到交换机的静态路由。

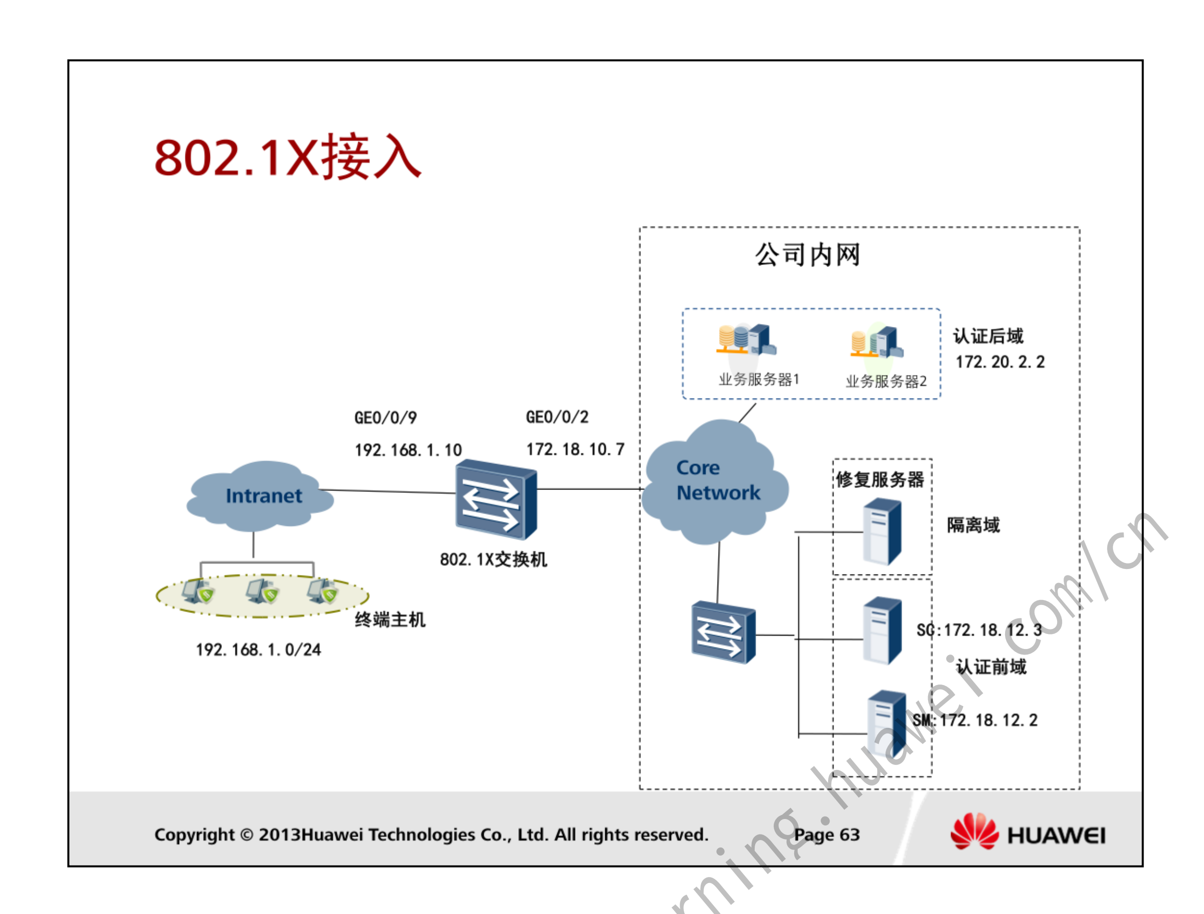


目录



  HUAWEI

- 本节主要介绍终端安全系统802.1X接入方式部署。



- 802.1X接入控制拓扑，IP及端口规划如图所示，交换机型号为S5300。



- 按照该流程图完成802.1X接入控制流程图。

增加设备

- 配置路径：接入控制策略 > 接入设备 > 接入设备 > 设备，单击“增加”
- 配置说明：
  - 组名称：默认
  - 设备类型：华为Quidway系列
  - RADIUS认证密钥：123456
  - RADIUS计费密钥：123456

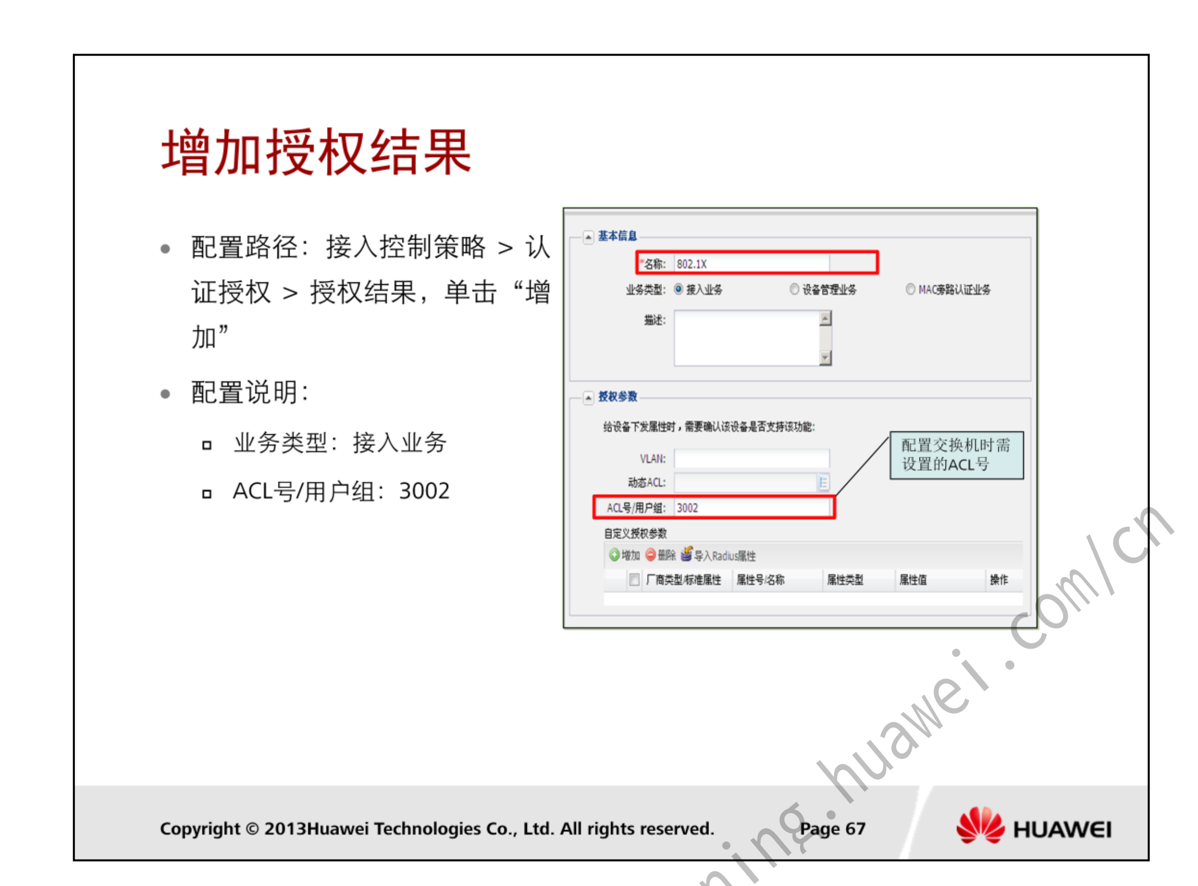
增加设备
设备基本信息
*名称: 802.1X
*组名称: 默认
*IP地址: 172.18.10.7
设备类型: 华为Quidway系列
*RADIUS认证密钥: ••••••
*RADIUS计费密钥: ••••••
实时计费周期(分钟): 1
描述:
启用Portal
确定 关闭







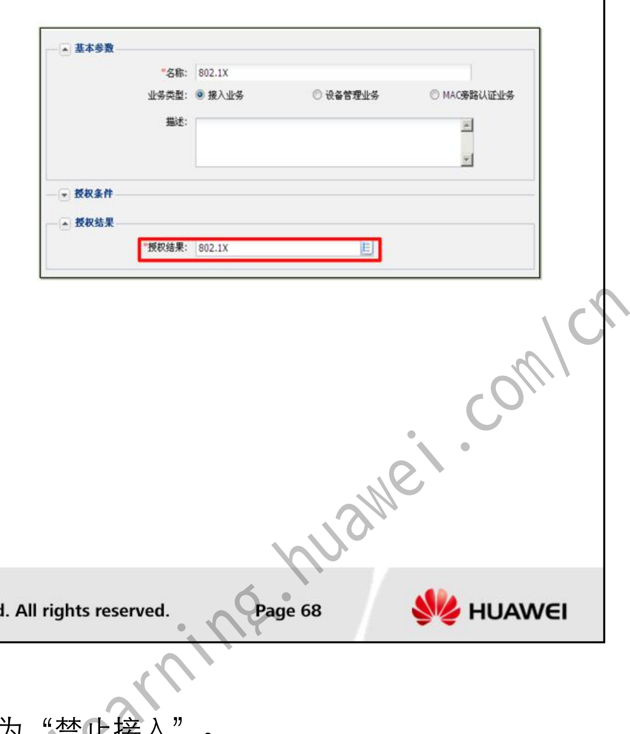
- 注意选择认证协议时必须保证交换机也支持该协议。



- 交换机也需配置ACL 3002，以识别策略中心下发的ACL 3002。
- 基于动态ACL的802.1X准入控制方案的实现原理是：根据终端用户的身份和终端主机的安全检查结果，安全控制器向交换机下发相应的ACL。由于不同厂商的交换机要求RADIUS服务器下发的RADIUS属性不同，为确保安全控制器（即RADIUS服务器）能够向交换机下发正确的ACL参数，要选择正确的设备类型，相关对应关系请查阅产品文档。

增加授权规则

- 配置路径：接入控制策略 > 认证授权 > 授权规则，单击“增加”
- 配置说明：
  - 业务类型：接入业务
  - 部门：研发部
  - 接入设备组：默认
  - 授权结果：802.1X



- 将默认授权规则的“授权结果”修改为“禁止接入”。

802.1X交换机配置思路

- 配置思路
  - 配置RADIUS服务器模板。
  - 配置RADIUS授权服务器。
  - 配置认证方案和计费方案。
  - 配置域，并绑定域和已配置的RADIUS服务器模板、认证方案及计费方案。
  - 启用全局和接口的802.1X认证。
  - 配置ACL规则。 在交换机配置该ACL规则，以便策略管理中心向交换机下发ACL时，交换机能够识别该ACL。



- 基础配置如接口配置省略，可查看相应型号版本的交换机产品文档。

配置RADIUS服务器模板

- 配置RADIUS服务器模板。

<Quidway> **system-view**

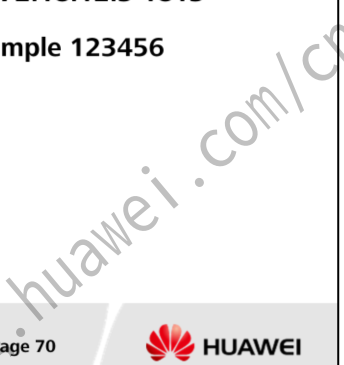
[Quidway] **radius-server template policy**

[Quidway-radius-policy] **radius-server authentication 172.18.12.3 1812**

[Quidway-radius-policy] **radius-server accounting 172.18.12.3 1813**

[Quidway-radius-policy] **radius-server shared-key simple 123456**

[Quidway-radius-policy] quit



- Radius模板配置：
  - 配置RADIUS认证服务器的IP地址，认证端口是1812。

    [Quidway] radius-server template policy

  - 配置计费服务器的IP地址，认证端口是1813。

    [Quidway-radius-policy] radius-server authentication 172.18.12.3 1812

  - 配置认证密钥和计费密钥为123456。

    [Quidway-radius-policy] radius-server accounting 172.18.12.3

    [Quidway-radius-policy] radius-server shared-key simple 123456

    [Quidway-radius-policy] quit

配置RADIUS授权服务器及认证计费方案

- 配置RADIUS授权服务器

  [Quidway] radius-server authorization 172.18.12.3 shared-key simple 123456

- 配置认证方案和计费方案

  [Quidway] aaa

  [Quidway-aaa] authentication-scheme auth

  [Quidway-aaa-authen-auth] authentication-mode radius

  [Quidway-aaa] accounting-scheme acco

  [Quidway-aaa-accounting-acco] accounting-mode radius



- 配置RADIUS授权服务器
  - 配置RADIUS授权服务器的地址，共享密钥是123456。

    [Quidway] radius-server authorization 172.18.12.3 shared-key simple 123456

- 配置认证方案和计费方案
  - 配置认证方案auth

    [Quidway-aaa] authentication-scheme auth

  - 认证方法为radius。

    [Quidway-aaa-authen-auth] authentication-mode radius

  - 配置计费方案acco

    [Quidway-aaa] accounting-scheme acco

    [Quidway-aaa-accounting-acco] accounting-mode radius

    [Quidway-aaa-accounting-acco] accounting realtime 1

    [Quidway-aaa-accounting-acco] quit

配置域及802.1X认证

- 配置域

  [Quidway-aaa] **domain default**

  [Quidway-aaa-domain-default] **radius-server policy**

  [Quidway-aaa-domain-default] **authentication-scheme auth**

  [Quidway-aaa-domain-default] **accounting-scheme acco**

- 配置802.1X认证

  [Quidway] **dot1x enable**

  [Quidway] **dot1X authentication-method eap**

  [Quidway-GigabitEthernet 0/0/9] **dot1x enable**

  [Quidway-GigabitEthernet 0/0/9] **dot1x port-method MAC**



- 配置域
  - 绑定已配置RADIUS服务器模板

    [Quidway-aaa-domain-default] radius-server policy
  - 绑定认证方案

    [Quidway-aaa-domain-default] authentication-scheme auth
  - 绑定计费方案

    [Quidway-aaa-domain-default] accounting-scheme acco

配置设备的ACL规则

- 配置ACL规则

  [Quidway] **acl 3002**

  [Quidway-acl-adv-3002] **rule 1 permit ip destination 172.18.12.3 0**

  [Quidway-acl-adv-3002] **rule 2 permit ip destination 172.18.12.2 0**

  [Quidway-acl-adv-3002] **rule 3 permit ip destination 172.20.2.2 0**

  [Quidway-acl-adv-3002] **rule 4 deny ip destination any**

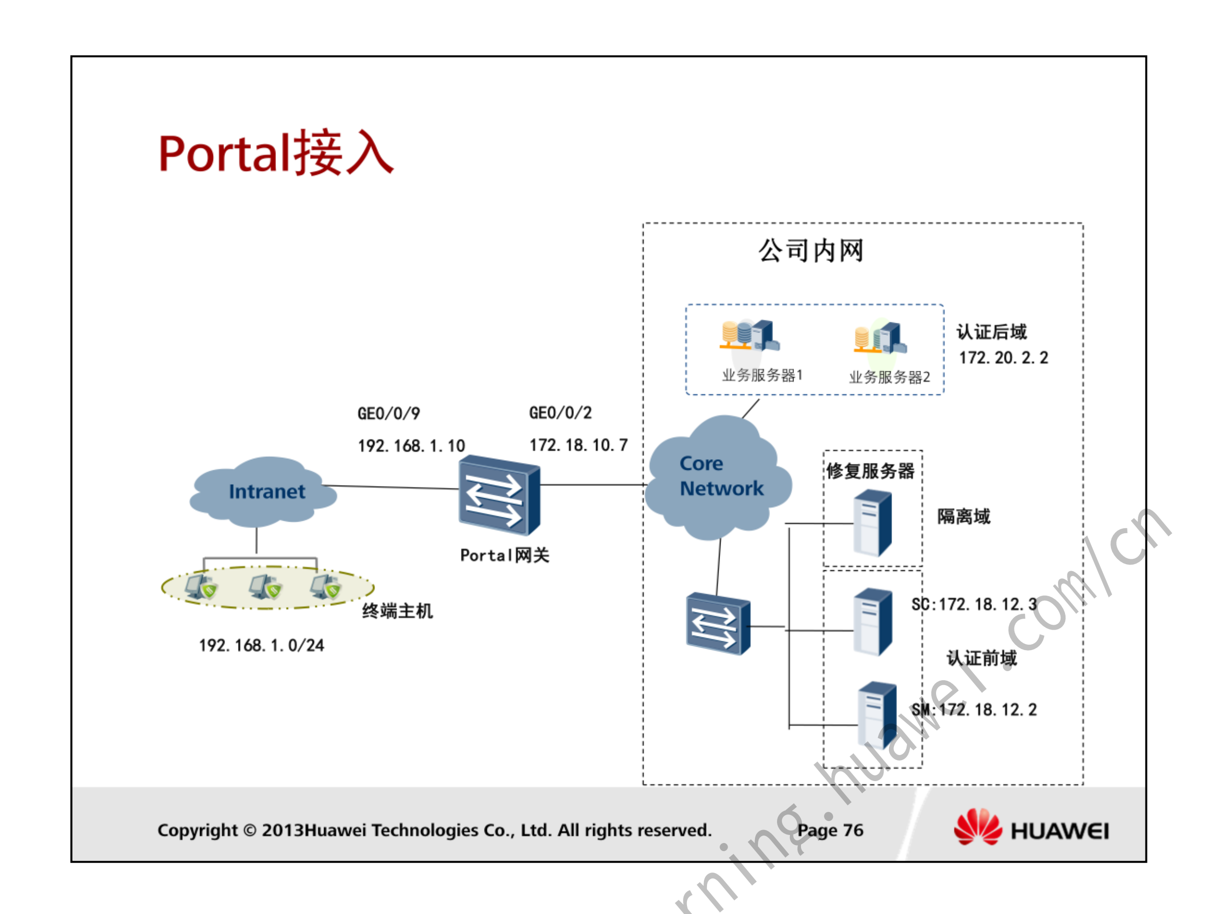




目录



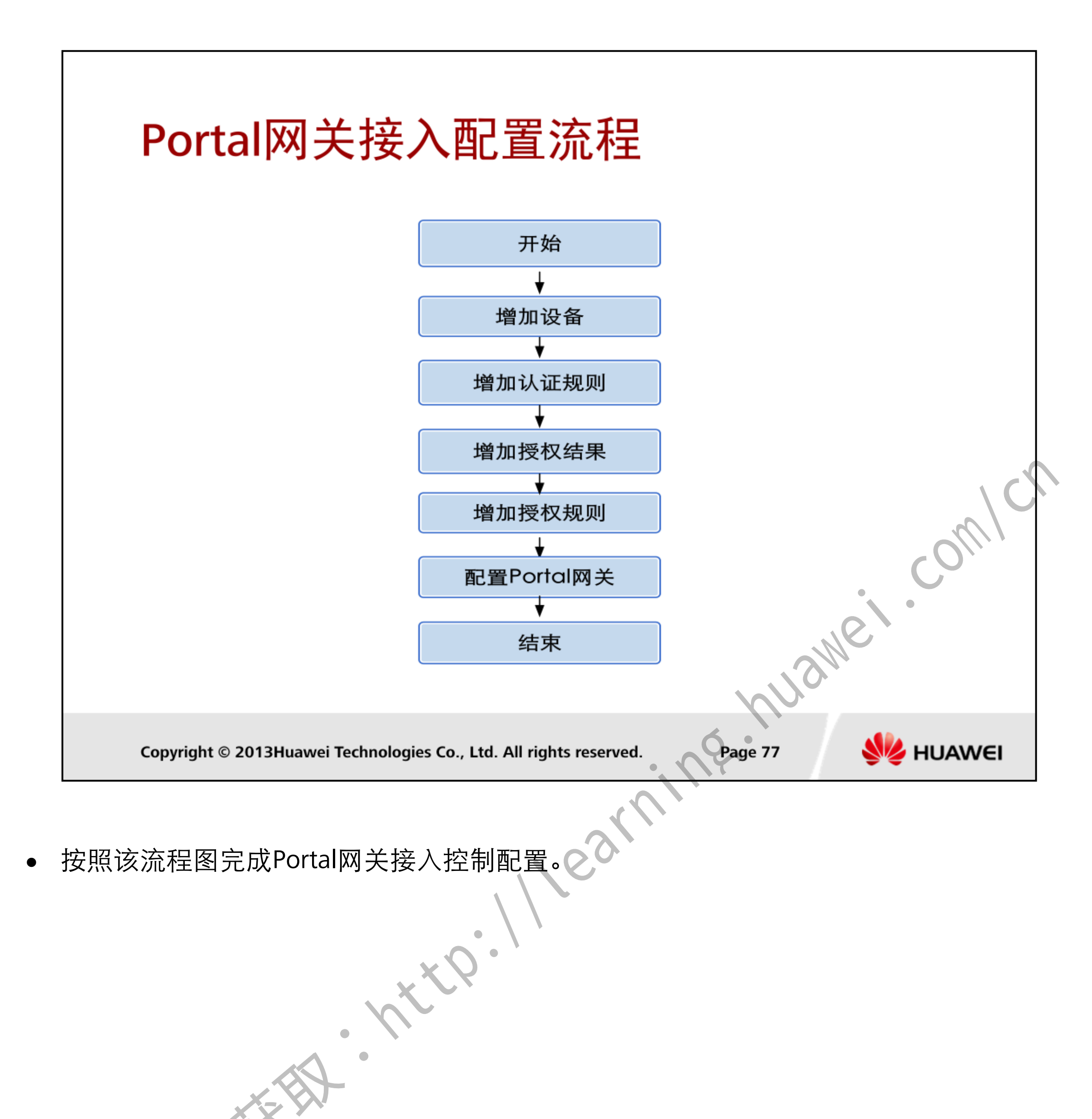
- 本节主要介绍Portal接入控制方式部署。



某企业采用所示的组网，终端设备通过二层交换机接入Quidway S5300交换机。

在现行组网结构的基础上，该企业部署策略管理中心，希望根据终端设备的安全检查结果进行接入控制，实现如下需求：以Quidway S5300交换机作为与策略管理中心联动的网络接入设备,在未进行认证的情况下，管理员只允许用户访问策略管理中心，禁止访问业务系统。 认证通过后，研发部员工能够访问业务系统，其余部门员工仍然不能访问业务系统。

如果终端用户没有安装NAC Agent，在终端用户通过Web浏览器访问业务系统时，Quidway S5300交换机自动向终端用户推送安全控制器的认证页面，方便终端用户通过Web方式进行认证。

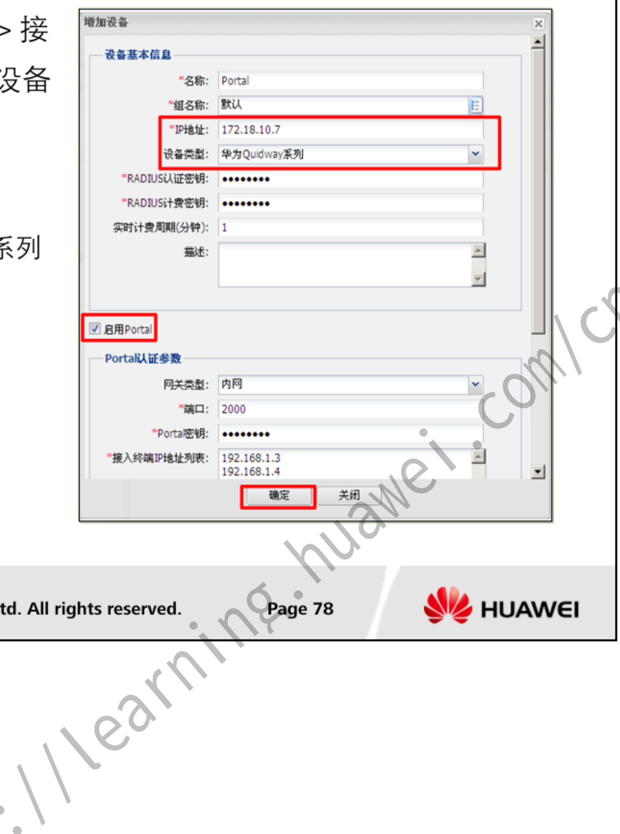


- 按照该流程图完成Portal网关接入控制配置。



增加设备

- 配置路径：接入控制策略 > 接入设备 > 接入设备管理 > 设备，单击“增加”
- 配置说明：
  - 设备类型：华为Quidway系列
  - 启用Portal
  - Portal密钥：password





- RADIUS认证密钥：password
- RADIUS计费密钥：password
- 接入终端IP地址列表：192.168.1.3 192.168.1.4

增加认证规则

- 配置路径：接入控制策略 > 认证授权 > 认证规则”，单击“增加”
- 配置说明：
  - 业务类型：接入业务
  - 部门：研发部
  - 接入设备组：默认
  - 认证协议：EAP-PEAP-MSCHAPv2协议

基本参数
*名称：Portal
业务类型：接入业务 设备管理业务 MAC旁路认证业务
描述：
认证条件
单击 展开可配置部门、接入设备组等
认证信息
启动RADIUS中继
*数据源：本地数据源
默认的认证协议：EAP-MD5协议
兼容老版本代理
*请选择允许使用的认证协议：PAP协议
CHAP协议
EAP-MD5协议
EAP-PEAP-MSCHAPv2协议
EAP-TLS协议
EAP-PEAP-GTC协议



增加授权结果

- 配置路径：接入控制策略 > 认证授权 > 授权结果，单击“增加”
- 配置说明：
  - 业务类型：接入业务
  - ACL号/用户组：3002







增加授权规则

- 配置路径：接入控制策略 > 认证授权 > 授权规则，单击“增加”
- 配置说明：
  - 业务类型：接入业务
  - 部门：研发部
  - 接入设备组：默认
  - 授权结果：Portal



- 将默认授权规则的“授权结果”修改为“禁止接入”。

Portal网关配置思路

- 配置思路
  - 配置交换机接口的VLAN。
  - 配置RADIUS服务器模板。
  - 配置RADIUS授权服务器。 RADIUS授权服务器负责向交换机下发COA消息，更新终端主机的ACL。在本例中，RADIUS授权服务器应配置为安全控制器（角色是Portal服务器）。
  - 配置认证方案和计费方案。
  - 配置域，并绑定域和已配置的RADIUS服务器模板、认证方案及计费方案。
  - 配置Portal认证服务器。 将安全控制器配置为Portal认证服务器。
  - 配置放行用户在认证前需要访问的网络资源，并配置ACL规则。



- 接口VLAN的配置省略。

配置RADIUS服务器模板

- 创建RADIUS服务器模板：

  [Quidway] **radius-server template policy**

  [Quidway-radius-policy] radius-server authentication 172.18.12.3 1812

  [Quidway-radius-policy] **radius-server accounting 172.18.12.3 1813**

  [Quidway-radius-policy] **radius-server shared-key simple password**

- 配置RADIUS授权服务器：

  [Quidway] **radius-server authorization 172.18.12.3 shared-key simple password**



- RADIUS模板配置
  - 创建服务器模板policy。

    [Quidway] radius-server template policy
  - 配置RADIUS认证服务器的IP地址和端口。

    [Quidway-radius-policy] radius-server authentication 172.18.12.3 1812
  - 配置计费服务器的IP地址和端口。

    [Quidway-radius-policy] radius-server accounting 172.18.12.3 1813
  - 配置认证密钥和计费密钥为password。

    [Quidway-radius-policy] radius-server shared-key simple password
- 配置RADIUS授权服务器。
  - 配置RADIUS授权服务器的IP地址，共享密钥配置为password，password为安全控制器与Quidway S5300交换机的授权密钥，必须与计费密钥、认证密钥保持一致。

    [Quidway] radius-server authorization 172.18.12.3 shared-key simple password

配置认证方案和计费方案

- 配置认证方案和计费方案。

[Quidway] **aaa**

[Quidway-aaa]**authentication-scheme auth**

[Quidway-aaa-authen-auth] **authentication-mode radius**

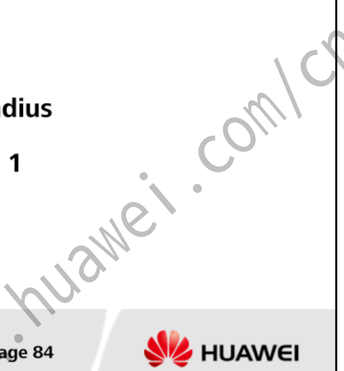
[Quidway-aaa-authen-auth] **quit**

[Quidway-aaa]**accounting-scheme acco**

[Quidway-aaa-accounting-acco] **accounting-mode radius**

[Quidway-aaa-accounting-acco] **accounting realtime 1**

[Quidway-aaa-accounting-acco] **quit**



- 配置认证方案和计费方案
  - 配置认证方案auth

    [Quidway-aaa]authentication-scheme auth
  - 认证方法为radius

    [Quidway-aaa-authen-auth] authentication-mode radius
  - 配置计费方案acco

    [Quidway-aaa]accounting-scheme acco
  - 计费模式设为radius

    [Quidway-aaa-accounting-acco] accounting-mode radius
  - 启用实时计费并设置计费间隔为1min

    [Quidway-aaa-accounting-acco] accounting realtime 1

配置域

- 配置域：

  [Quidway-aaa] **domain default**

  [Quidway-aaa-domain-default] **radius-server policy**

  [Quidway-aaa-domain-default] **authentication-scheme auth**

  [Quidway-aaa-domain-default] **accounting-scheme acco**

  [Quidway-aaa-domain-default] **quit**

  [Quidway-aaa] **quit**



- 配置域：
  - 配置域default

    [Quidway-aaa] domain default
  - 绑定RADIUS服务器模板

    [Quidway-aaa-domain-default] radius-server policy
  - 绑定认证方案

    [Quidway-aaa-domain-default] authentication-scheme auth
  - 绑定计费方案

    [Quidway-aaa-domain-default] accounting-scheme acco

配置Portal认证服务器

- 配置Portal认证服务器：

```
[Quidway] web-auth-server server1
[Quidway-web-auth-server-server1] server-ip 172.18.12.3
[Quidway-web-auth-server-server1] port 50200
[Quidway-web-auth-server-server1] shared-key simple password
[Quidway-web-auth-server-server1] url http://172.18.12.3:8080/webauth
[Quidway-web-auth-server-server1] quit
[Quidway] interface vlanif 105
[Quidway-Vlanif105] web-auth-server server1
[Quidway-Vlanif105] quit
```



HUAWEI

- 配置Portal认证服务器：
  - 配置服务器IP地址

    [Quidway] web-auth-server server1

    [Quidway-web-auth-server-server1] server-ip 172.18.12.3
  - 配置Portal认证服务的端口号

    [Quidway-web-auth-server-server1] port 50200
  - 配置Portal认证服务器与交换机交互的共享密钥

    [Quidway-web-auth-server-server1] shared-key simple password
  - 配置Portal认证服务器对应的URL

    [Quidway-web-auth-server-server1] url http://172.18.12.3:8080/webauth
  - 在接口下绑定Portal认证服务器

    [Quidway] interface vlanif 105

    [Quidway-Vlanif105] web-auth-server server1

配置认证前需访问的资源及ACL规则

- 配置放行用户在认证前需要访问的网络资源，并配置ACL规则

  [Quidway] **portal free-rule 0 destination ip 172.18.12.2 mask 255.255.255.255**

  [Quidway] **portal free-rule 1 source ip 172.18.12.2 mask 255.255.255.255**

  [Quidway] **acl 3002**

  [Quidway-acl-adv-3002] **rule 1 permit ip destination 172.20.2.2 0**

  [Quidway-acl-adv-3002] **rule 2 deny ip destination any**

  [Quidway-acl-adv-3002] **quit**





- 配置放行用户在认证前需要访问的网络资源，并配置ACL规则，配置Portal认证服务器时，已经配置了安全控制器，交换机会自动放行访问安全控制器的数据流，无需管理员手工配置。 配置Free Rule，放行用户在认证前需要访问的网络资源（此处是DNS服务器172.18.12.2）。

  [Quidway] portal free-rule 0 destination ip 172.18.12.2 mask 255.255.255.255

  [Quidway] portal free-rule 1 source ip 172.18.12.2 mask 255.255.255.255

- 配置放行业务系统的规则（ACL 3002）

  [Quidway] acl 3002

  [Quidway-acl-adv-3002] description postauthentication

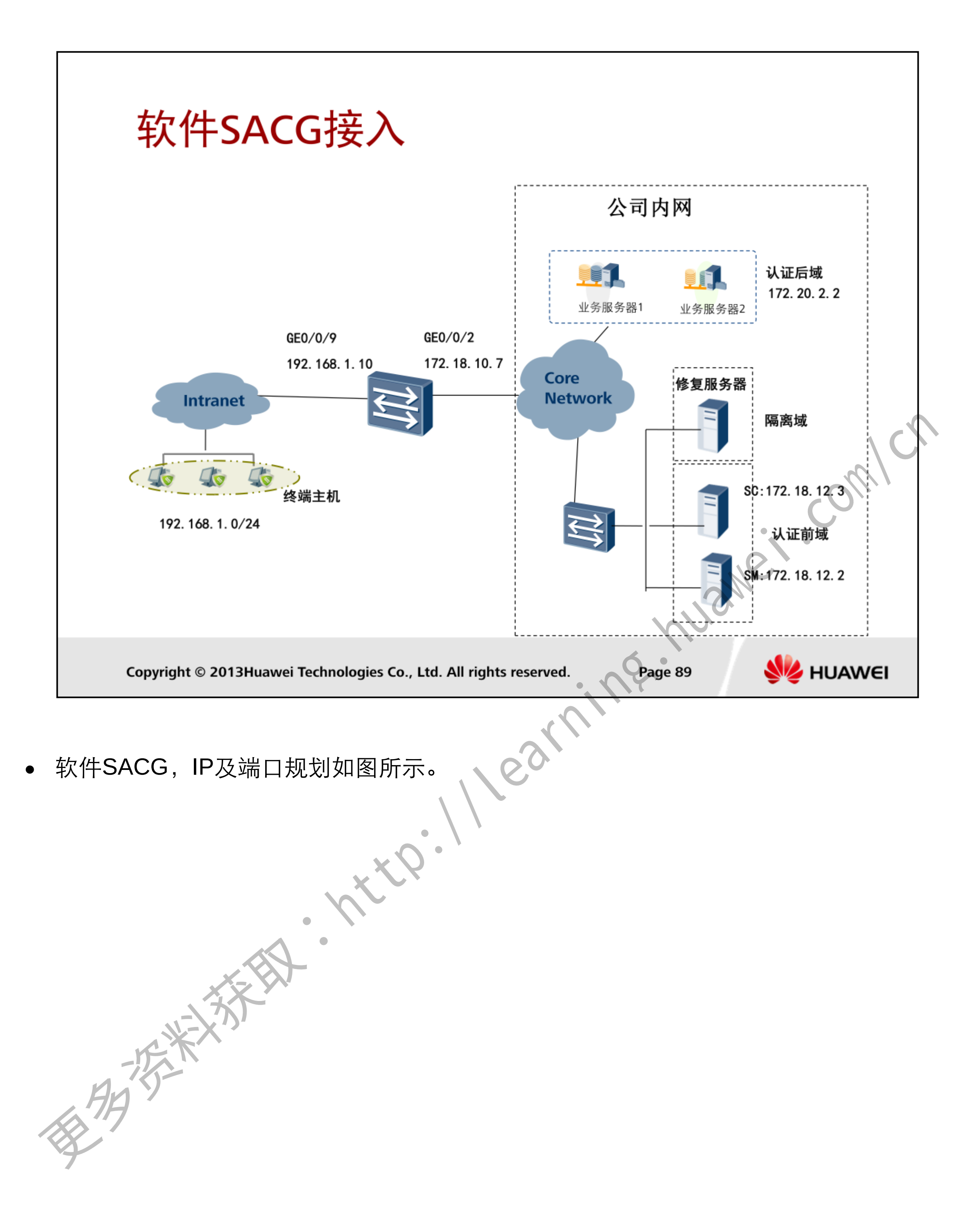
  [Quidway-acl-adv-3002] rule 1 permit ip destination 172.20.2.2 0

  [Quidway-acl-adv-3002] rule 2 deny ip destination any

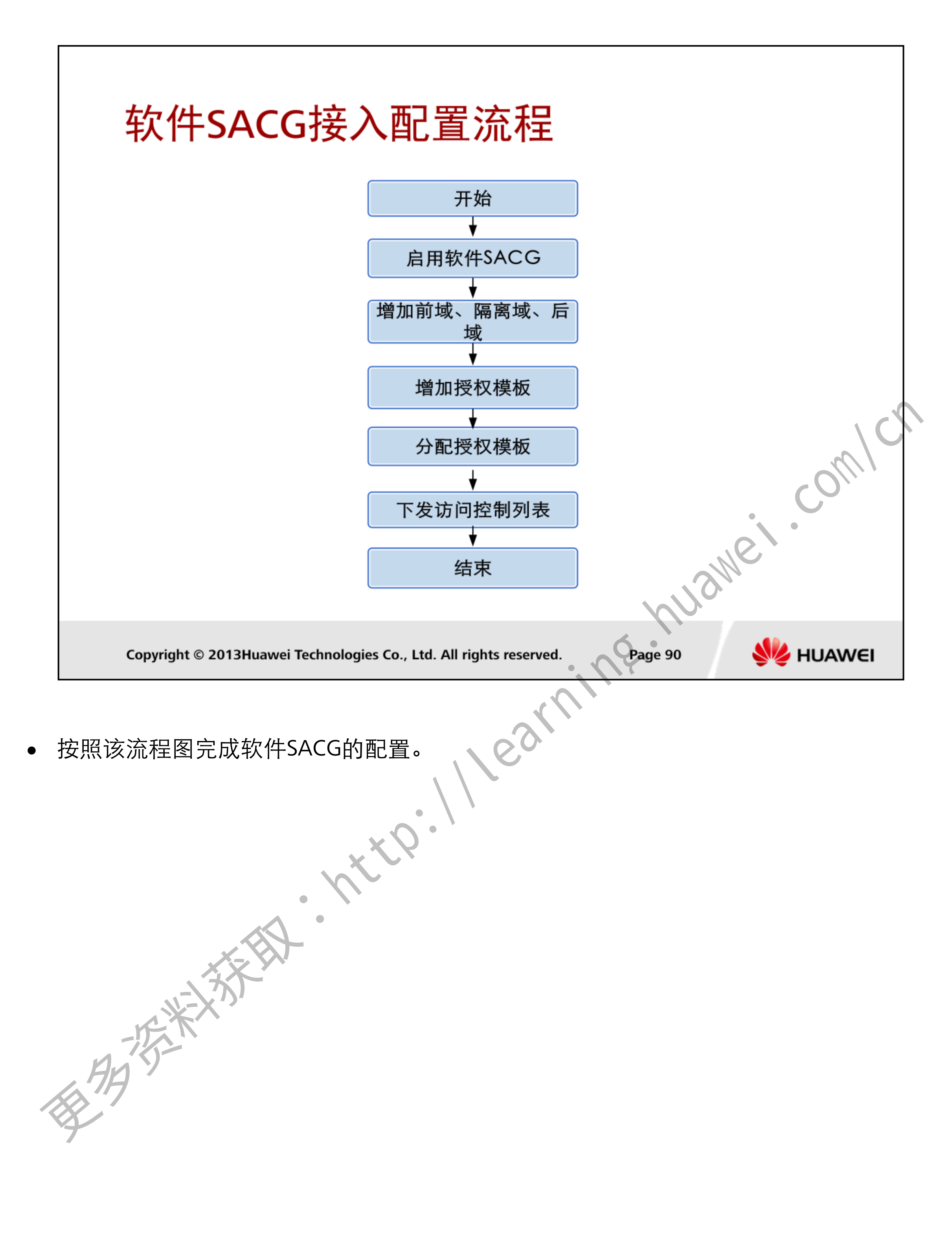




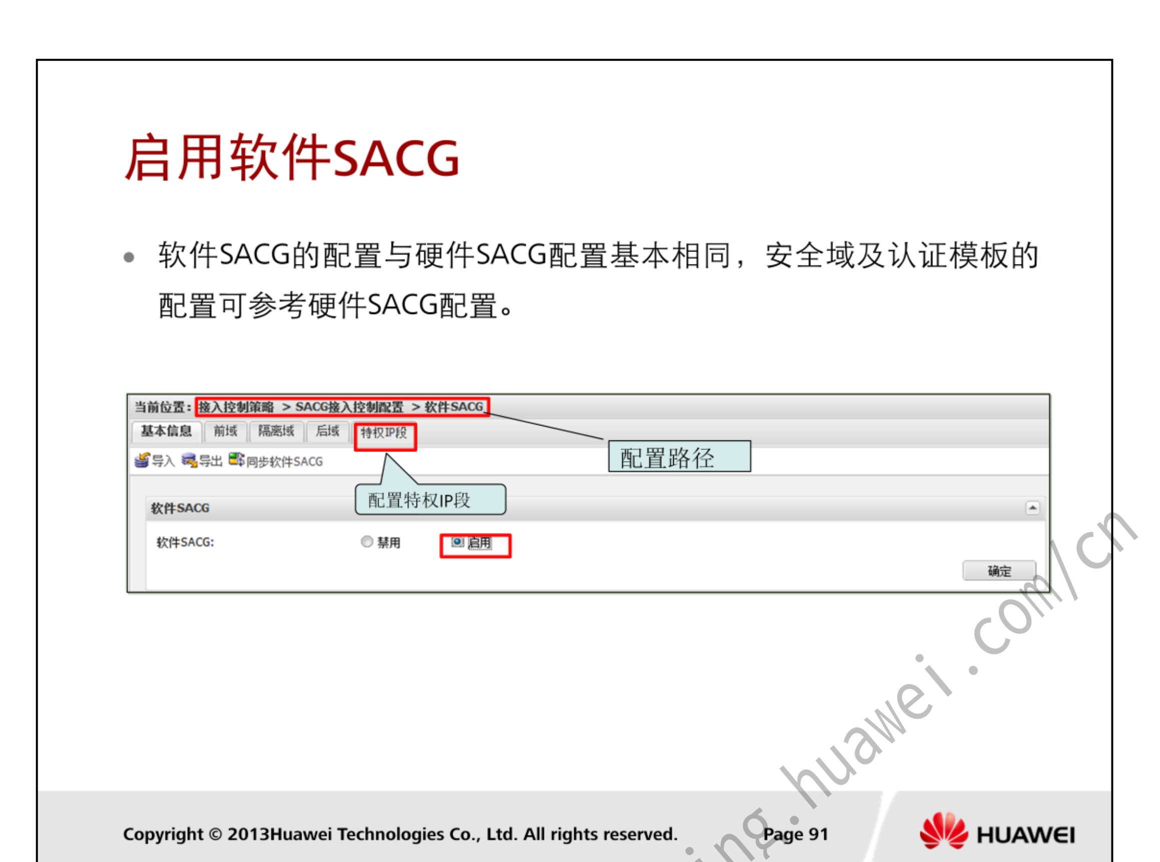
- 本节主要介绍软件SACG接入控制方法。



- 软件SACG，IP及端口规划如图所示。



- 按照该流程图完成软件SACG的配置。



要使用软件安全接入控制网关实施终端主机的接入控制功能，终端用户必须安装并通过代理接入受控网络。Web客户端和Web Agent插件认证方式不支持软件安全接入控制功能。



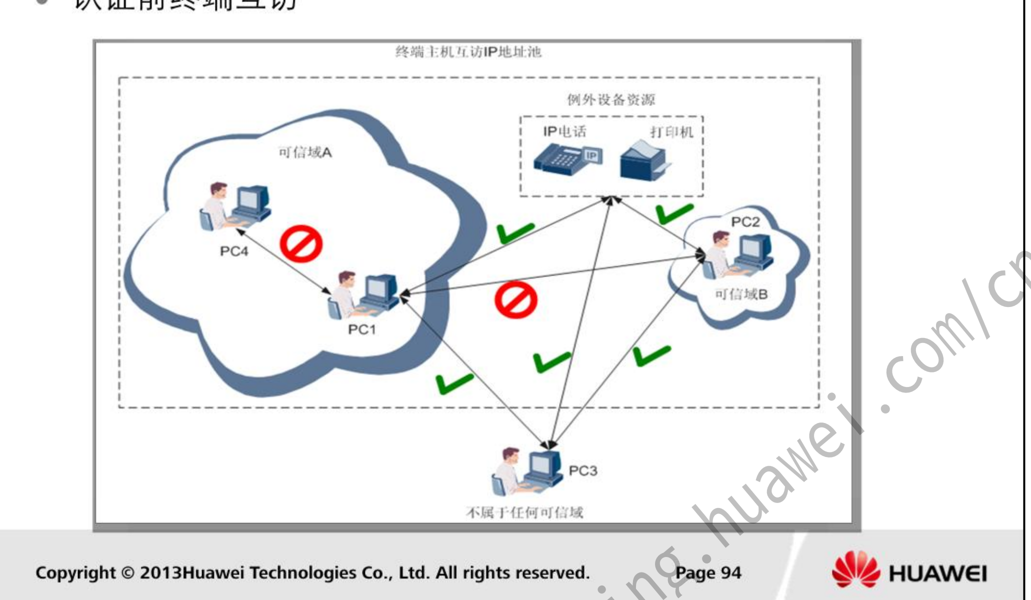
为了使控制器不限制某些特权终端用户访问认证后域中的网络资源，管理员需要将该终端用户的IP地址加入特权IP地址池。



目录



- 本节主要介绍终端互访控制概念、原理及配置。



可信域是一个逻辑的概念，用来确定网络中可以互相共享资源的范围。可信域需要应用于部门、网络区域或账号才能生效。而可信域的优先级别从部门、网络区域和账号依次从低到高。只有在高优先级的可信域没有设置的情况下，低优先级的可信域设置才会生效，对于部门的可信域而言，如果账号没有单独设置可信域， 则自动继承所属部门的可信域设置。可信域适用于允许所指定的终端主机之间互相访问，而不允许来自可信域以外的终端主机访问可信域中的任意终端主机（例如，禁止普通员工访问财务部所在的网络）。

认证前终端互访规则：属于同一个可信域的终端主机及属于不同可信域的终端主机不允许互相访问，例外设备不受可信域影响。例外设备是那些不能安装代理的终端设备如IP电话、打印机等。

终端主机互访控制是基于软件的方式，解决硬件安全接入控制网关在终端主机互访控制力度不足的问题，硬件安全接入控制网关部署于接入层，在终端主机数量较多的情况下，需要部署的硬件安全接入控制网关的数量会增多，导致成本增加，硬件安全接入控制网关部署于汇聚层或核心层，终端主机之间互访的流量不经过硬件安全接入控制网关，导致硬件安全接入控制网关无法控制终端主机之间的互访。

终端主机互访控制

- 认证后终端互访

终端主机互访IP地址池
例外设备资源
IP电话
打印机
可信域A
PC4
PC1
PC2
可信域B
PC3
不属于任何可信域

HUAWEI

- 终端互访控制原理：管理员在管理器配置终端主机互访控制的访问控制列表，并下发至代理。当终端主机要互相访问时：
  - 对于IP地址不在终端主机互访控制IP地址池的终端主机PC3，不受终端主机互访控制机制限制。无论PC3的终端用户是否通过安全检查，PC3均能够访问位于可信域的PC1、PC2和例外设备资源。
  - 在启用终端主机互访控制功能的情况下，PC1和PC4两台终端主机属于同一个可信域，则如果PC1或PC4其中一台终端主机未通过安全检查（例如PC1没有安装代理），则PC1与PC4之间不能互相访问。
  - 如果PC1或PC4两台终端主机都通过安全检查，则PC1与PC4之间允许互相访问。
  - 在启用终端主机互访控制功能的情况下，PC1和PC2两台终端主机位于两个不同的可信域，则无论PC1和PC2的终端用户是否通过安全检查，PC1与PC2之间不能互相访问

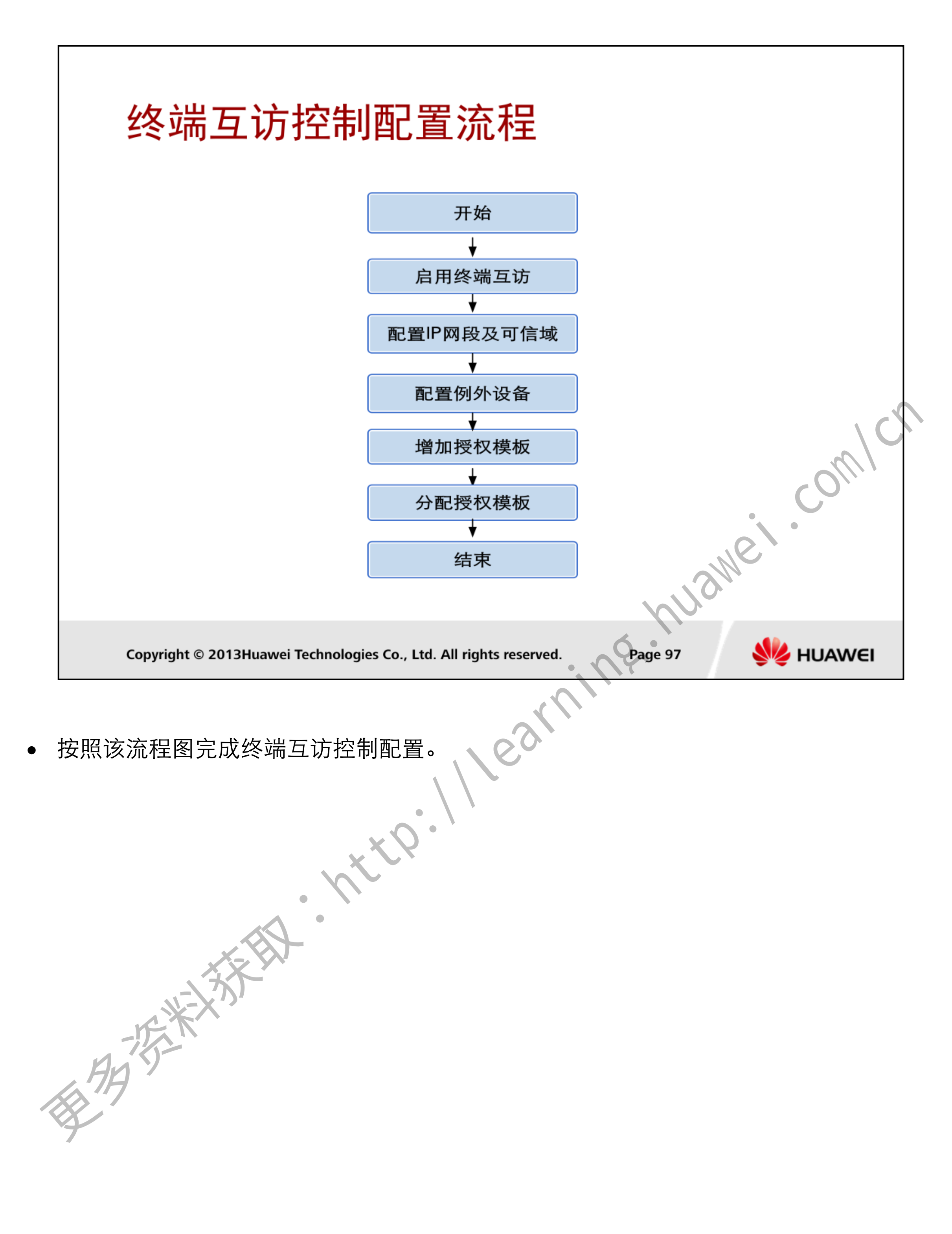
在终端主机互访控制IP地址池中，不适合启用终端主机互访控制功能的设备（如IP Phone、打印机），可加入例外设备资源，确保终端用户能够访问例外设备和以及例外设备能够访问网络。一些公共类的设备为所有终端用户使用，管理员需要将这些例外资源应用至所有的部门或所有的网络区域。例外设备资源必须应用于部门、网络区域或账号才能生效。如果某些例外设备资源需要供所有终端用户，必须在所有的部门或网络区域应用该例外设备资源。

软件SACG与终端主机互访控制冲突处理原则

- 当两种控制方式出冲突时，现安全管理器将会遵循以最小权限的原则进行处理，安全控制器同时实施软件安全接入控制网关和终端主机互访控制两者的访问控制列表。
- 所谓的最小权限原则是指在同时启用软件安全接入控制和终端主机互访控制，对于某个特定的IP地址：
  - 如果软件安全网关禁止访问该IP地址，则终端主机无法访问该IP地址。
  - 如果软件安全接入控制网关允许访问该IP地址，同时终端主机互访控制要求实施只有互相信任的终端主机才允许互相访问，则终端主机需要遵循终端互访控制的访问控制列表才能与该IP地址进行通信。



- 软件安全接入控制网关与终端主机互访控制同时生效时，下列组合方式在出现冲突时均遵循最小权限原则进行处理：
  - 软件安全控制网关的认证前域+终端主机互访控制
  - 软件安全控制网关的隔离域+终端主机互访控制
  - 软件安全接入控制网关的认证后域+终端主机互访控制
- 举例:
  - 对于软件安全接入控制网关而言，认证后域为10.1.1.1和10.1.1.10。终端主机PC1和10.1.1.1在可信域1，而10.1.1.10在可信域2，考虑到最小权限的原则，PC1的终端用户在通过安全检查后只有访问10.1.1.1，不能访问10.1.1.10。



- 按照该流程图完成终端互访控制配置。

启动终端控制及逃生通道

配置路径

当前位置：接入控制策略 > SACG接入控制配置 > 终端互访控制

基本信息 终端互访IP段 可信域 例外设备资源

导入 导出 同步终端互访控制

终端互访控制

终端互访控制: 禁用 启用

确定

设置逃生通道

逃生通道: 禁用 启用

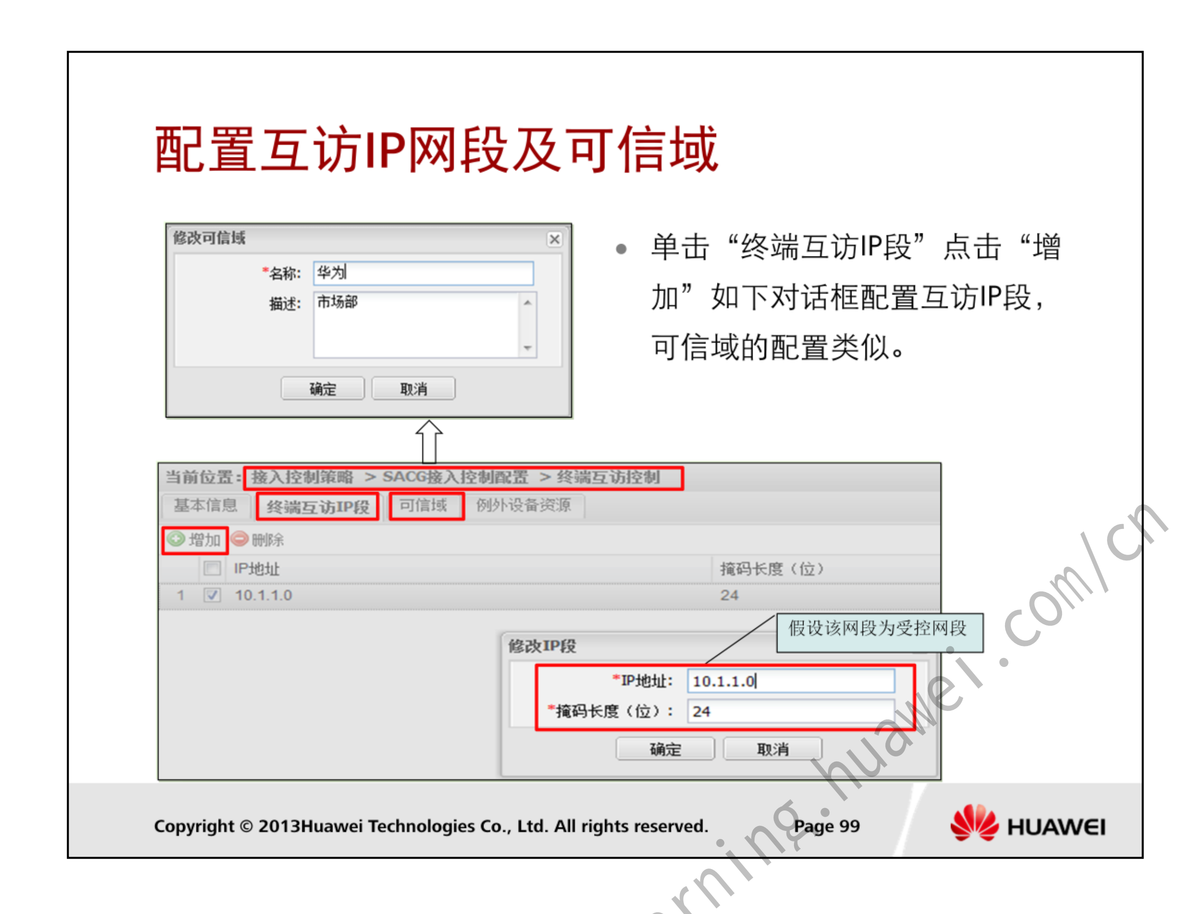
确定

  HUAWEI

终端主机互访控制涉及的逃生通道，是指代理在所属归属地所有的控制器都失效后，终端主机互访控制机制自动失效，代理对所有的终端主机互访请求都会予以放行。

提供逃生通道的目的在于，当归属地所有的控制器都失效后，代理对所有的终端主机互访请求都会予以放行，确保网络畅通，业务不被因控制器故障而被中断。

在逃生通道开启的情况下，如果控制器从故障中恢复，则逃生通道自动关闭，终端主机互访控制机制自动启动。



- 终端主机互访控制IP地址池是指终端主机互访功能生效的地址段。从终端主机互访控制的角度看，企业网络可划分为两个区域：
  - 实施终端主机互访控制的区域
  - 不实施终端主机互访控制的区域
- 两个区域之间的终端主机允许互相访问。
- 实施终端主机互访控制的区域由管理员配置的一系列IP地址或IP地址段组成，称之为终端主机互访控制IP地址池。终端主机互访控制机制的规则如下：
  - 如果两台终端主机的IP地址都在终主机互访控制IP地址池中，则终端主机互访控制机制生效，两台终端主机之间能否互相访问受到终端主机互访控制功能的限制
  - 如果两台终端主机的IP地址都不在终主机互访控制IP地址池中，则终端主机互访控制机制不生效，两台终端主机之间能否互相访问不会受到终端主机互访控制功能的限制。
  - 如果一台终端主机的IP地址在终主机互访控制IP地址池中，而另一台终端主机的IP地址不在终主机互访控制IP地址池中，则终端主机互访控制机制不生效，两台终端主机之间能否互相访问不会受到终端主机互访控制功能的限制。
  - 在终端主机互访控制IP地址池中，两台终端主机之间是否能够互相访问，取决于两台终端主机是否属于同一个可信域，并且是否都通过安全检查，

配置列外设备

- 配置路径：接入控制策略>SACG接入控制配置>终端互访配置，单击“例外设备”标签，单价“增加”。



所谓例外设备资源，是指IP地址在终端主机互访控制IP地址池中，但不对该设备或资源实施终端主机互访控制。

在可信域中代理允许终端用户访问例外设备资源，而不要求例外设备资源安装代理或者通过身份认证或安全认证。例外设备资源适用于无法安装代理的场合，例如打印机、IP Phone或者不适合安装代理的软件服务器，代理对任何终端主机访问例外设备资源都是放行的，无论终端主机是否通过安全检查



- 注意：选择相应的可信域和例外设备。



- 分配授权规则模板到研发部。



总结

1. Policy center的安装过程需注意那几个步骤?
2. 数据库安装需注意的步骤有哪些?
3. 简述硬件SACG的配置部骤
4. 简述802.1X交换机的配置思路





思考题

- 终端互访控制如何实现?
- 终端互访逃生通道作用是什么?
- 配置Portal网关接入时控制及计费模板的作用是什么?





练习题

- 判断题
  1. Policy Center操作系统Server2003不需要安装SP2补丁。
- 多选题
  1. 部署接入控制时，控制策略可以分配给?

     A.部门

     B.账号

     C.IP段

     D.区域



- 习题与答案:
  - 判断题答案：错误
  - 多选题答案：ABC

Thank you

www.huawei.com

HC120320004
终端安全系统操作与运维管理

www.huawei.com

HUAWEI



目标

- 学完本课程后，您将能够:
  - 掌握终端安全系统的运营管理操作；
  - 掌握终端安全系统维护配置；
  - 熟悉常用运维管理工具的使用；

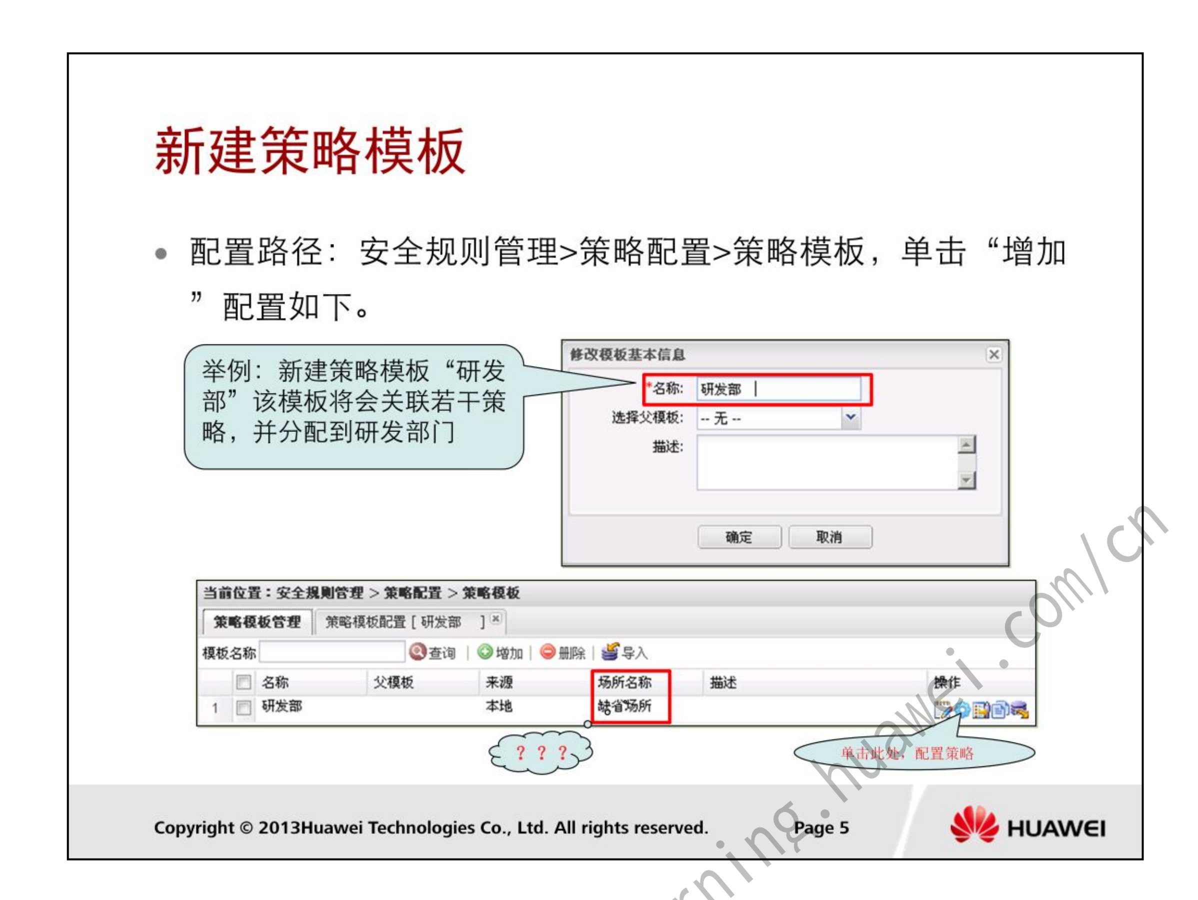




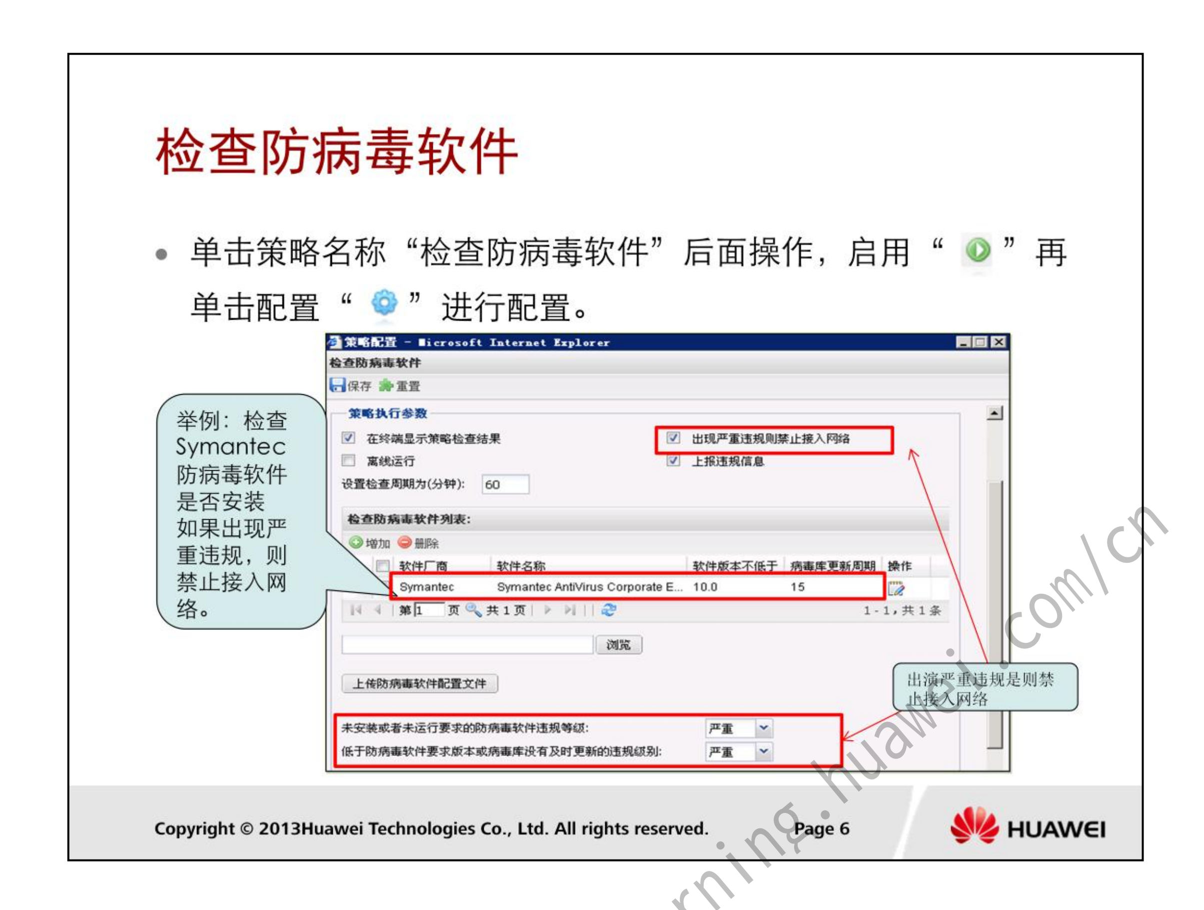
- 本节介绍与策略管理功能相关的界面操作，以及以具体举例介绍如何配置策略管理业务，以便实现终端主机安全管理和终端用户行为审计。



- 在安装完安全管理器之后，安全管理器不包含任何策略。管理员必须上传策略后，才能通过创建策略模板向终端用户下发策略，上传安全策略需注意以下几点：
  - 修改策略的名称或策略包的名称，将导致上传至安全管理器的策略不可用。请勿修改策略的名称或策略包的名称。
  - 当局点部署了管理中心时，安全管理器所上传的策略必须与管理中心所上传的策略兼容，管理中心才能向安全管理器成功下发策略模板。
  - 如果上传策略失败，请在安全管理器的“系统配置 > 服务器配置 > FTP服务器配置”检查FTP服务器的参数是否还没进行配置。如果FTP服务器的参数已经配置，则请检查并确保FTP服务器的参数是正确的，再尝试上传策略。



- 策略模板
  - 策略模板是若干策略的集合，为了审计不同终端主机的安全状况和终端用户的行为，管理员需要定制不同的策略模板用于保护和管理终端主机。当终端用户进行身份认证和安全检查时，NAC Agent执行与终端用户相关联的策略模板中的所有策略。
  - 创建策略模板的前提条件：数据库处于正常运行状态、管理器处于正常运行状态、管理员已经成功登录管理器、管理员已经将策略上传至管理器、管理员拥有增加策略模板的操作权限。
- 场所：
  - 场所是指终端用户使用终端安全系统接入受控网络办公时的终端环境,随着网络的发展，终端用户的办公场所越来越多样化，有些员工在公司内办公，有些员工在家里办公，而有些员工长期出差，办公地点不确定。同时，终端用户接入网络的方式也各有不同，例如：通过局域网、无线网络、VPN等方式接入。在进行策略管理时，如果不考虑终端用户的场所，将可能导致在不同场所下终端用户不能正常接入受控网络办公。
  - 策略中心默认只支持缺省场所。缺省场所是指没有定义使用场合的场所，表示不区分终端用户的使用场合，当按场所进行策略管理业务时，组织需要根据自己的需求联系华为技术有限公司工程师定制相应的场所文件。例如，定制在线和离线场所。获取到场所文件后，管理员需要在管理器导入场所文件。



- 该策略检查终端主机是否安装指定的防病毒软件。如果终端主机已经安装防病毒软件，该策略检查防病毒软件的程序版本号、病毒库是否及时更新、防病毒软件是否运行。如果终端主机未安装指定的防病毒软件，或防病毒软件不符合条件，Agent代理将会记录终端主机的相关信息，并将违规信息上报至数据库，供管理员查阅。
- 检查类的策略主要还有：
  - 检查操作系统补丁
    - 该策略检查终端主机是否已经安装Microsoft Windows操作系统对应的补丁。如果终端主机未安装对应版本的补丁程序，NAC Agent将记录该操作系统的相关信息，并上报至安全控制器，供管理员查阅。
  - 检查注册表配置
    - 介绍检查注册表配置策略的参数配置过程，及注册表键值与Microsoft Windows防火墙状态、Microsoft Windows自动播放的关系，供配置注册表策略参数时参考。
  - 检查屏保设置
    - 检查终端主机的屏幕保护设置是否符合要求。如果终端用户未启用屏幕保护功能，或屏保设置不符合要求，则该策略的检查结果为违规
  - 检查文件共享
    - 检查终端文件共享的账号以及权限是否符合要求，并提供自动修复功能。

检查屏保设置

- 单击策略名称“检查屏保设置”后面操作，启用“ ”再单击配置“ ”进行配置。

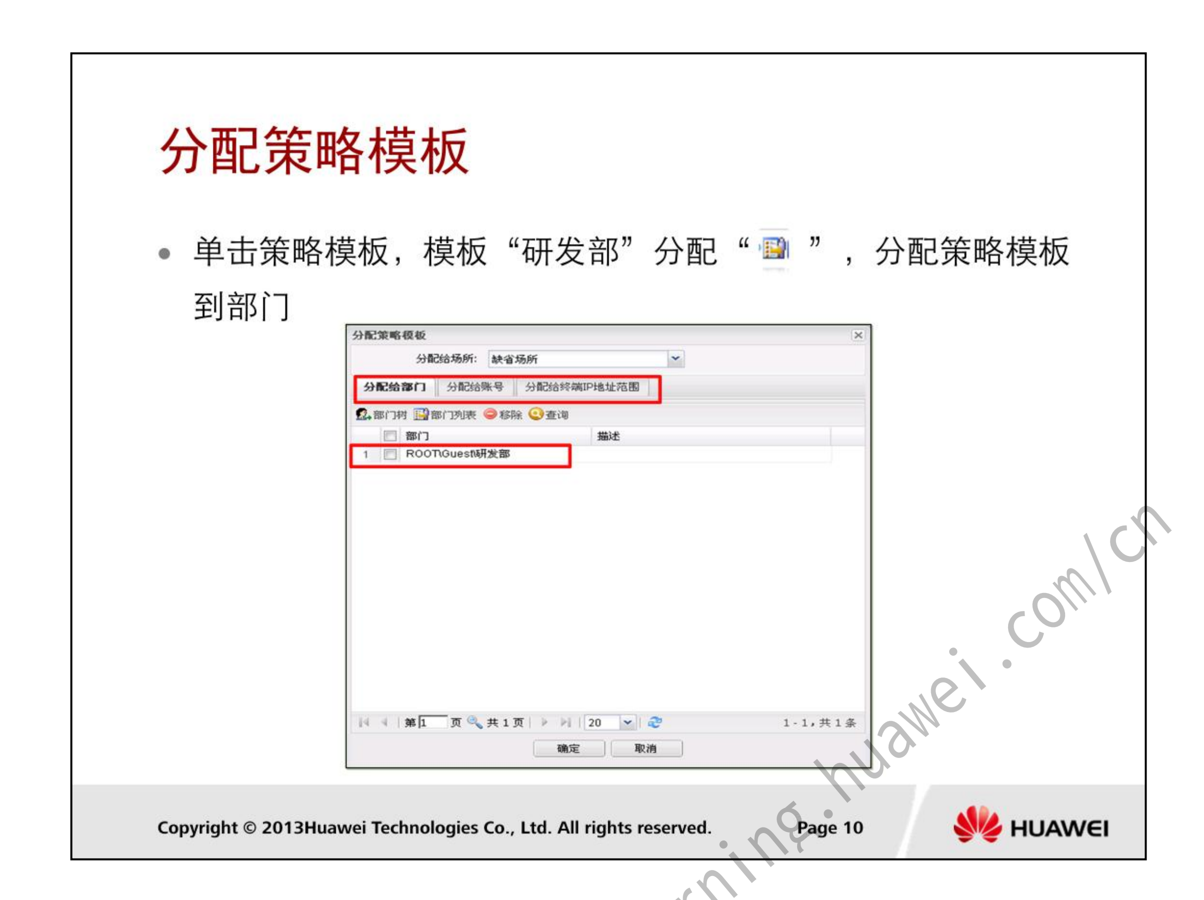
- 检查终端主机的屏幕保护设置是否符合要求。如果终端用户未启用屏幕保护功能，或屏保设置不符合要求，则该策略的检查结果为违规。
- 其他勾选项详细说明：
  - 在终端显示策略检查结果：设置是否允许在终端主机的代理界面上显示检查结果，选中此项，允许在终端主机的代理界面上显示检查结果，不选中此项，禁止在终端主机的Agnet代理界面上显示检查结果，该参数默认选中。
  - 出现严重违规则禁止接入网络：设置终端主机出现严重违规是否禁止接入网络，选中此项，当检查的违规等级为“严重”时，SC控制器将禁止终端主机接入网络，不选中此项，当检查的违规等级为“严重”时，SC控制器仍允许终端主机接入网络，该参数默认不选中。
  - 启用自动修设置终端主机出现违规是否启用自动修复。 选中此项，当终端主机出现违规时，Agent代理会自动修复其违规项，不选中此项，当终端主机出现违规时，代理不会自动修复其违规项，该参数默认选中。
  - 离线运行：设置是否在Agent代理离线运行时执行该策略。选中此项，表示在代理离线运行时执行该策略，违规信息将在认证通过后上报SC控制器，取消选中此项，表示在代理离线运行时不执行该策略。代理的离线运行状态包括以下情况
    - 终端主机未进行身份认证。
    - 终端主机进行身份认证，但身份认证失败。
    - 终端主机通过身份认证后，终端用户注销登录。



- 该策略检查是否允许通过指定的端口通信。当终端主机使用该端口通信时，Agent代理将阻止终端主机使用该端口进行通信，同时记录该应用程序的相关信息。违规信息将上报至数据库，供管理员查阅。
- 监控类策略主要有：
  - 监控DHCP设置
    - 该策略监控终端主机是否使用DHCP的方式获取地址。
  - 监控非法外连
    - 该策略监控终端主机是否非法连入互联网。当终端主机存在非法连入互联网的违规行为时，该策略可以阻断终端主机与违规代理服务器或网络的连接，并记录终端主机的违规信息，将违规信息上报至安全控制器，供管理员查阅。
  - 监控屏幕拷贝
    - 该策略提供禁止终端用户使用拷屏键的功能。如果终端用户使用“PrtSc”或“Alt+PrtSc”拷屏键截取屏幕，NAC Agent将会禁止终端用户截取屏幕的行为。
  - 监控访问站点
    - 该策略监控终端用户访问网站的行为。当终端用户访问设定的网站时，NAC Agent将根据预先设置的控制动作决定是否允许终端用户继续访问该网站，并记录该站点的相关信息。违规信息将上报至安全控制器，供管理员查阅。
  - 监控系统设备
    - 该策略设置是否允许终端用户使用系统设备（如打印机、蓝牙、红外、SD/MMC控制器等）。如果终端用户使用这些受控设备，NAC Agent将会记录终端用户使用这些受控设备的行为。违规信息将上报至安全控制器，供管理员查阅。



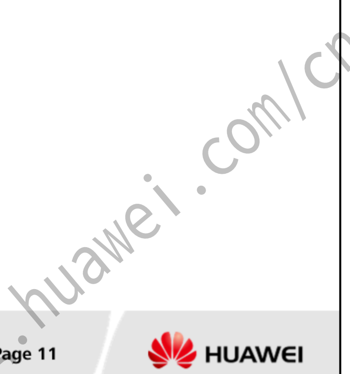
- 该策略监控终端主机是否非法连入互联网。当终端主机存在非法连入互联网的违规行为时，该策略提供阻断与违规代理服务器或网络的连接，并记录终端主机的违规信息，将违规信息上报至数据库，供管理员查阅。



- 应用策略模板是指将定制好的策略模板应用于某个部门，该部门会继承该策略模板的所有配置信息。为部门配置策略模板能够统计整个部门的终端安全状况，审计终端用户的行为。NAC Agent将会定期向安全控制器请求更新策略模板，根据更新后的策略参数确定何时开始执行策略，以检查终端主机的安全状况或审计终端用户的行为。
- 如果不同的策略模板分别应用到部门、账号和终端IP地址范围，则优先级最高者所分配到的策略模板将会生效。部门、账号、终端IP地址范围的优先级关系为：账号 > 终端IP地址范围 > 部门，不建议同时为部门和终端IP地址范围分配策略模板。



目录



HUAWEI

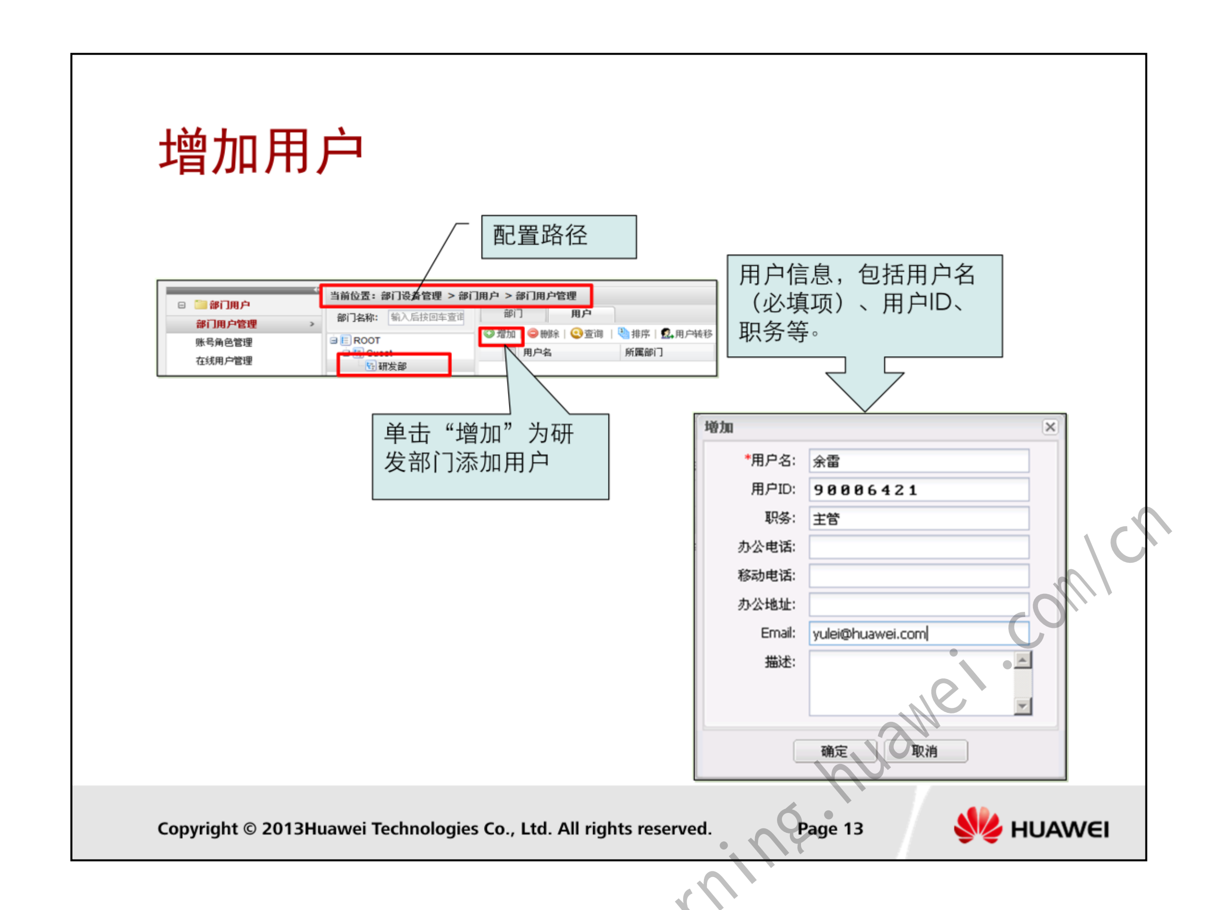
- 部门信息管理功能是为了方便管理员在管理器中建立企业的组织结构。管理器中的一个部门对应于企业中的一个部门。通过在管理器中维护部门中的信息，管理员能够集中管理部门信息、员工信息和资产信息。
- 管理终端用户是指管理员对企业或部门内部的员工信息进行集中维护和管理。当新员工加入部门时，管理员负责将员工的相关信息录入管理器。当员工的工作岗位发生调动时管理员需要修改员工信息。当员工辞职后，管理员需要删除该终端用户的信息。

部门用户管理

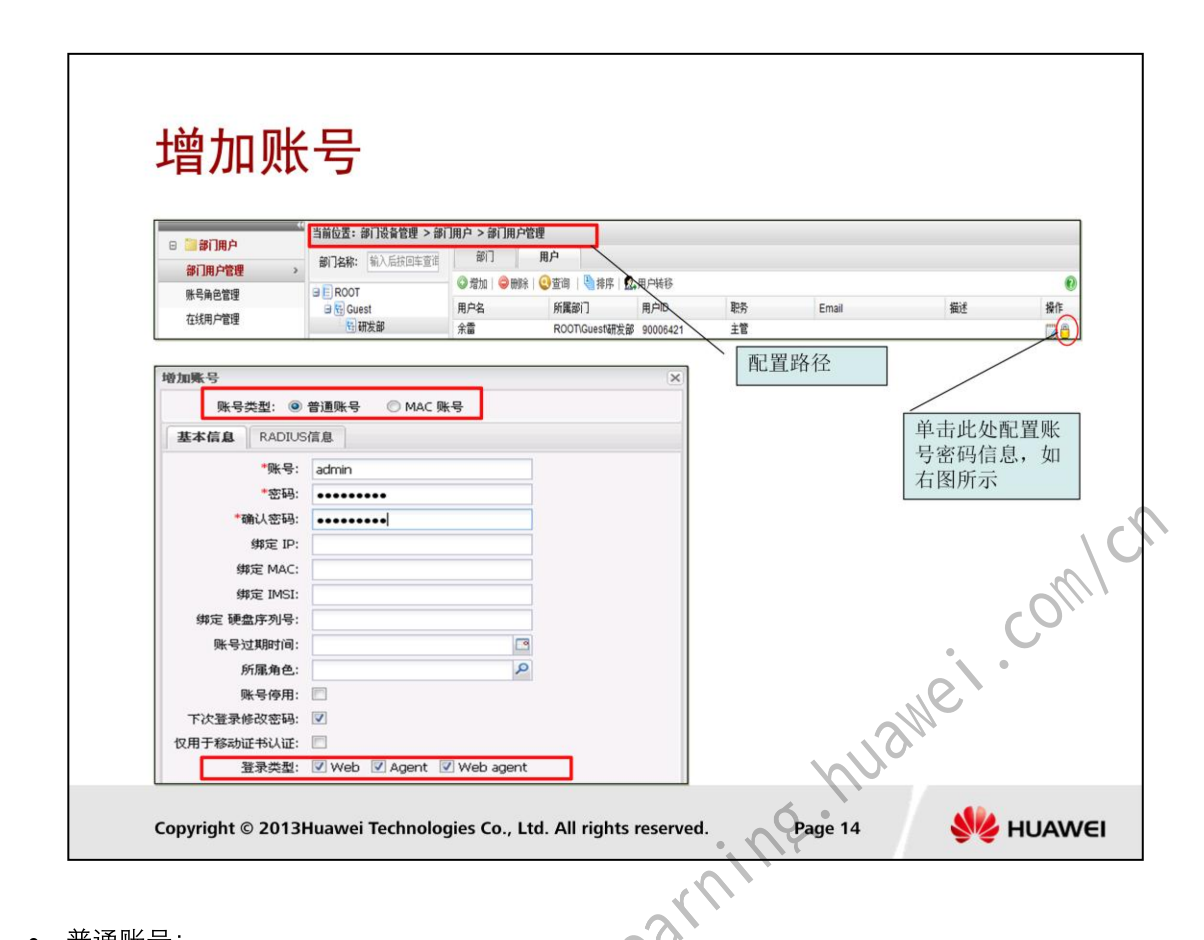
- 部门信息管理功能是为了方便管理员在安全管理器中建立企业的组织结构。安全管理器中的一个部门对应于企业中的一个部门。通过在安全管理器中维护部门中的信息，管理员能够集中管理部门信息、员工信息和资产信息。



- Policy Center支持通过部门来管理用户和账号信息。通过创建部门和导入部门信息2种方式能够增加部门。



- 通过创建终端用户和导入终端用户信息2种方式能够增加终端用户。
- 设置终端用户的ID，不能与已存在的终端用户ID重复，最大长度为50byte，由于安全管理器允许终端用户存在同名的情况，用户ID适用于通过姓名以外的方式唯一标识一个终端用户，例如终端用户的工号。



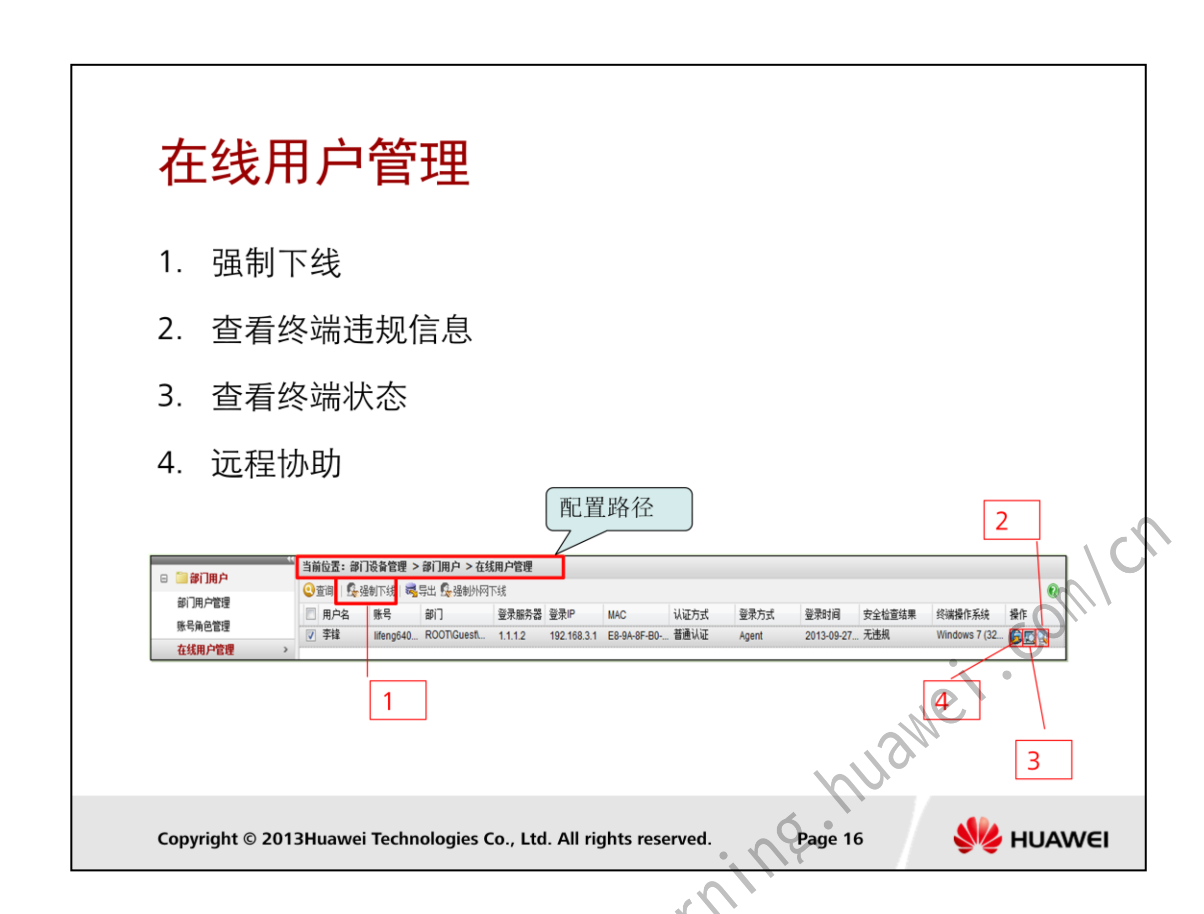
- 普通账号：
  - 普通账号是管理员在管理器的指定部门和指定终端用户下创建的账号，终端用户在认证时需要提供账号和密码，普通账号支持Agent代理、Web Agent插件和Web客户端三种认证方式。
- MAC账号：
  - MAC账号是管理员在管理器的指定部门和指定终端用户下利用终端主机的MAC地址创建的账号，终端用户必须在与MAC账号对应的终端主机上才能认证通过，MAC账号只支持Agent代理认证方式。
- 其他参数说明：
  - 绑定IP，设置终端用户是否只能使用当前账号从指定IP地址的终端主机进行身份认证。普通账号最多允许绑定10个IP地址，多个IP地址之间使用半角逗号分隔。
  - 绑定MAC，设置终端用户是否只能使用当前账号从指定MAC地址的终端主机进行身份认证。只有通过Agent代理方式接入受控网络的账号才支持MAC地址绑定功能。其中MAC地址的账号格式为“xx-xx-xx-xx-xx-xx”，“x”为“0～9”或“A～F”，表示十六进制数。
  - 账号过期时间，设置账号在什么时候过期，过期的账号将会失效，无法通过身份认证。
  - 账号停用，选择是否禁止该账号进行身份认证。只有普通账号和MAC地址账号才能支持账号停用功能。
  - 下次登录修改密码，设置该账号在下次登录时是否需要修改密码。
  - 仅用于移动证书认证，当该账号可以用于移动证书认证时，设置是否限制该账号只能用于移动证书认证，不能再使用其他认证方式。选中此项，表示限制该账号只能用于移动证书认证。

匿名用户管理

- 匿名认证是指终端用户不需要认证账号和密码，在指定的网络区域通过配置支持匿名认证的登录类型即可完成认证的一种认证方式,管理器自动创建一个名称为“～anonymous”的专用账号



- 匿名认证方式适用于组织机构在全局范围或局部范围内无须鉴别终端用户的身份，终端用户通过匿名方式进行认证的场合。例如，临时接入的终端用户数量较多，或者在开始推广终端安全系统阶段，管理员可能无法及时分发大量的账号而导致终端用户无法及时接入受控网络，进而影响终端用户办公。采用匿名认证能够降低管理员维护部门和账号信息的成本。对于终端用户，特别是访客，不需要申请和记忆特定的账号和密码，使得终端用户能够更容易、方便地通过认证，并接入到受控网络。
- 在安装策略中心时，管理器自动创建一个名称为“～anonymous”的专用账号。在默认情况下，“～anonymous”处于禁用状态。管理员通过启用匿名认证方式激活“～anonymous”账号。同时，代理、Web Agent插件和Web客户的认证方式列表自动增加匿名认证方式供终端用户选择。
- 与普通账号一样，管理员能够为“～anonymous”账号分配接入控制、策略模板、补丁模板、软件分发等业务，从而指定了匿名用户在访问受控网络时应遵循的安全规则，使得终端用户通过匿名认证方式接入内网后能够在权限范围内访问受控资源，避免没有合法权限的用户对受控网络的安全造成威胁。
- 由于匿名认证存在业务审计困难的特点，匿名认证通常需要在受限的环境中中使用，避免权利被滥用。管理员可以通过IP地址段开明确匿名认证适用的范围，确保在受信任的环境中才能适用匿名认证，其他范围依然启用身份认证。



- 管理器提供查询在线用户功能，能够帮助管理员从大量在线用户中快速定位在线的指定用户及账号的信息。



检查文件共享 (记录数:2)

共享名称	共享路径	访问权限控制	在线状态	检查时间	检查结果
软件	D:学习\软件	用户:EveryOne共有者权限非法,需删除	在线	2013-09-27 16:40:05	一般违规
新建文件夹	D:学习\软件\新建文件夹	用户:EveryOne共有者权限非法,需删除	在线	2013-09-27 16:40:05	一般违规

检查磁盘分区信息 (记录数:1)

分区类型	硬盘编号\逻辑盘符	分区编号\磁盘类型	分区类型描述	是否为引导分区	分区大小（MB）	在线状态	检查时间	检查结果
物理分区	1	4	Compaq config partition	否	15109	在线	2013-09-27 16:40:06	一般违规

检查防病毒软件 (记录数:1)

是否安装	违规描述	在线状态	检查时间	检查结果
否	您的电脑没有安装指定防病毒软件，建议安装：Symantec AntiVirus Corporate Edition	在线	2013-09-27 16:40:05	一般违规

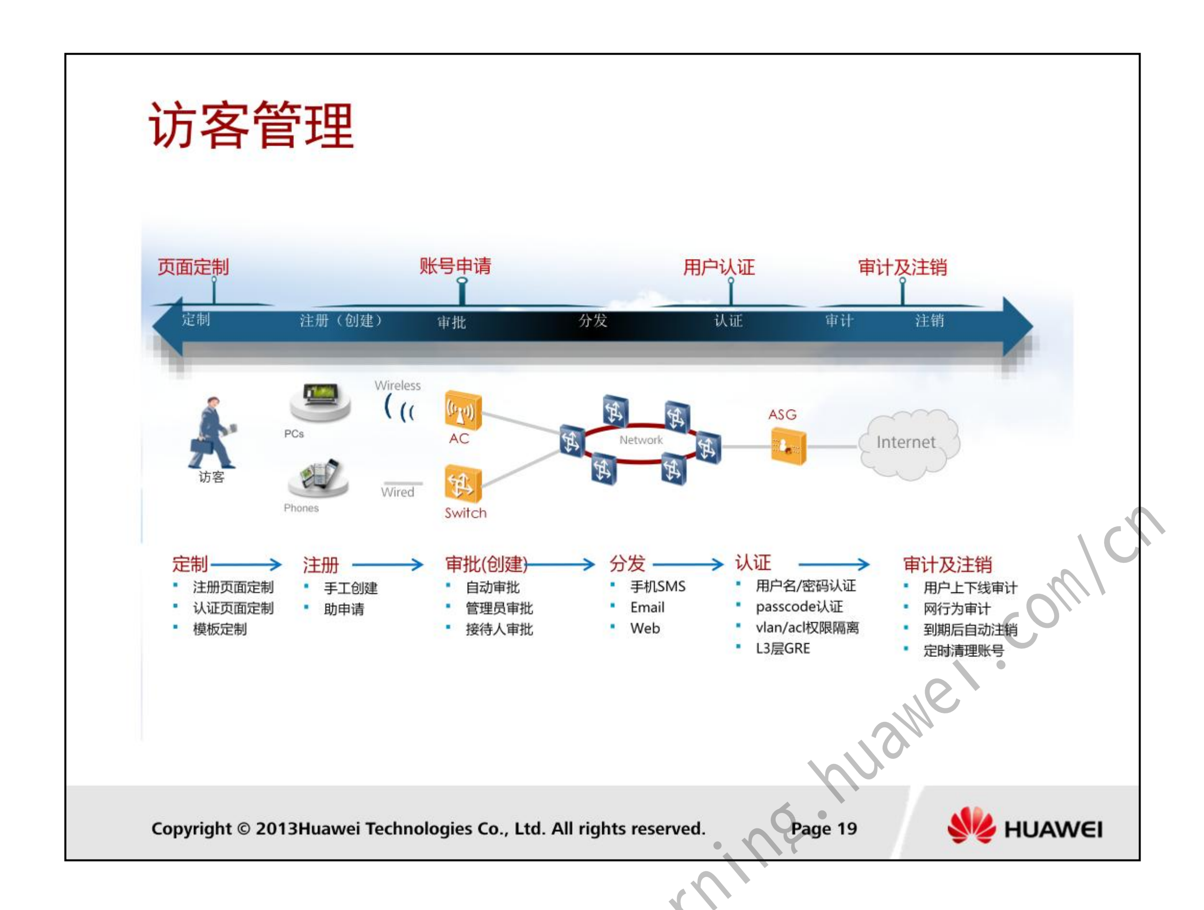
监控DHCP设置 (记录数:1)

是否设置DHCP	网卡信息	检查时间	在线状态	检查结果
否	MAC address: E8-9A-8F-B0-C6-B (IP Address:192.168.3.1);	2013-09-27 16:40:06	在线	一般违规

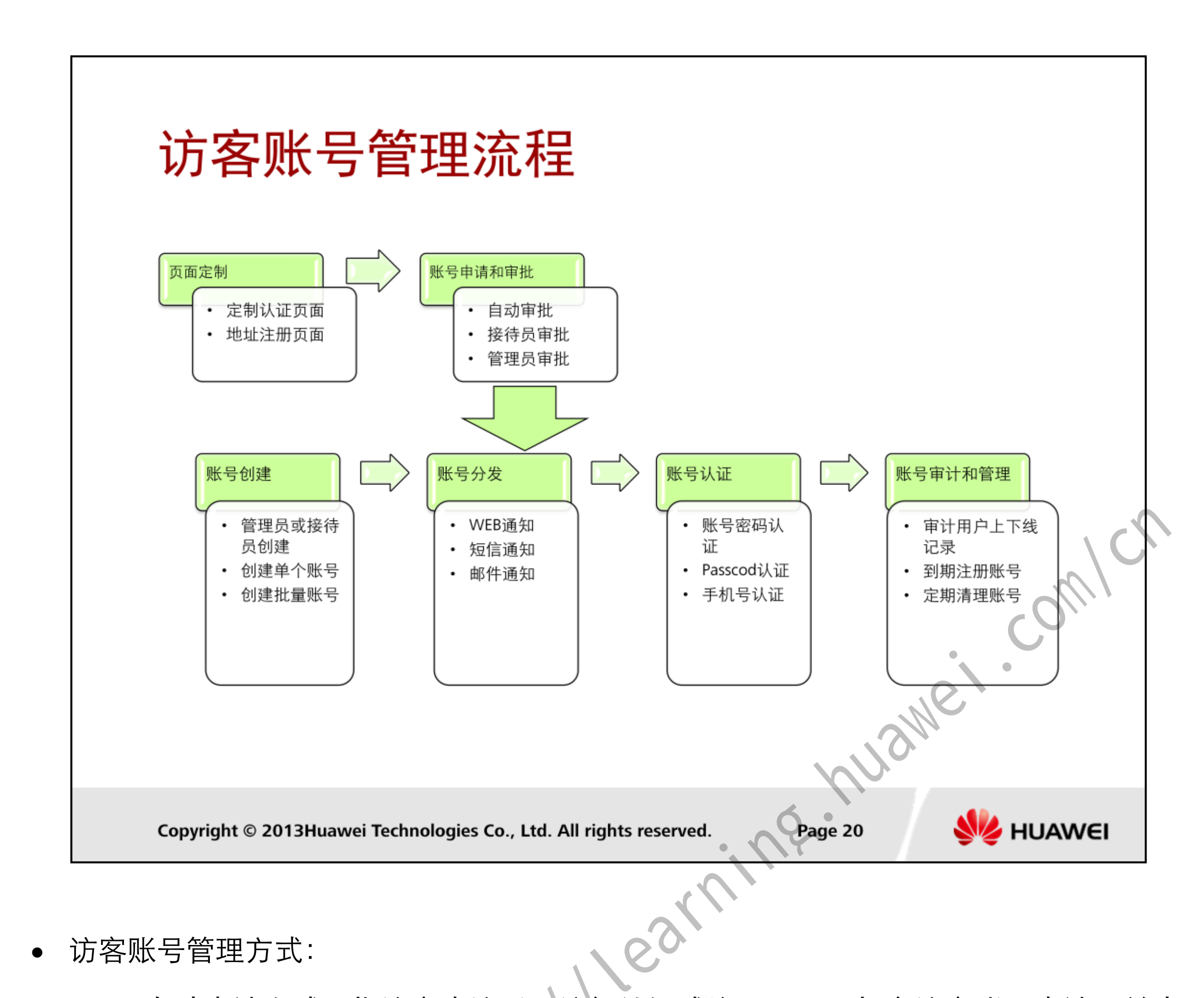
- 可以查看到终端违规情况



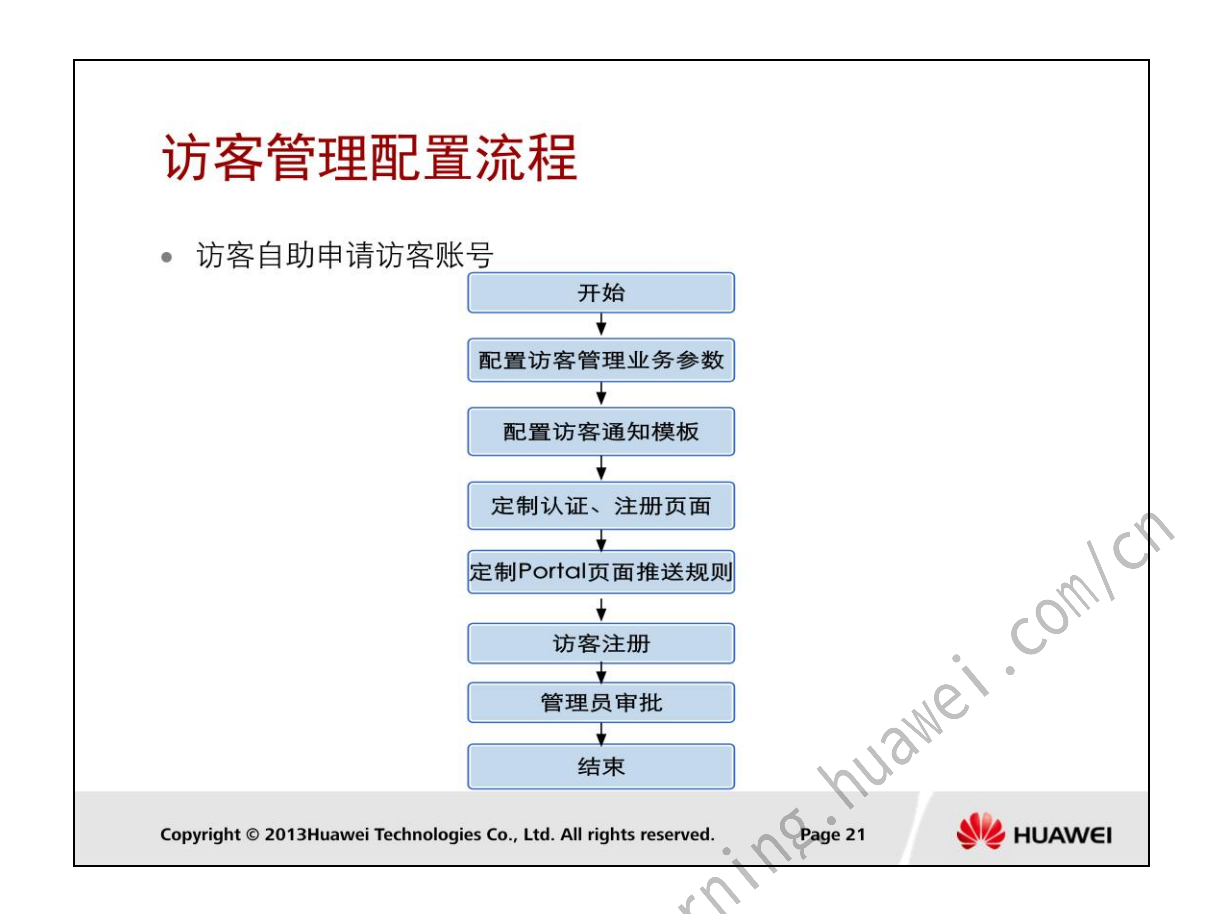
- 可查看终端用户、操作系统、内存、CPU等信息。



- 访客账号是组织机构专门为来访客人准备的账号，用于验证来访客人的身份是否合法。来访客人通常包括合作人员、客户等。访客账号通常为临时性账号，同时授予较低网络访问。
- 应用场景
  - 场景一：访客使用手机号快速注册账号：访客使用手机号提交账号申请，申请自动审批通过，快速获得密码，访客使用手机号和密码认证通过后即能接入网络。
  - 场景二：访客自助申请账号并经过审批：访客提交账号申请，待接待员工或管理员审批通过后，访客使用账号和密码认证通过后即能接入网络。
  - 场景三：接待员工创建访客账号：接待员工先创建好访客账号，访客来访后，接待员工将账号和密码通过邮件或短信通知访客，访客使用账号和密码认证通过后即能接入网络。
  - 场景四：自动生成并打印访客账号：用户在企业内部排队等待办理业务，企业为提升客户满意度为用户提供无线网络接入服务，用户在打印排号票时同时获得系统自动生成的访客账号，该账号是用户获取网络访问权限的凭证。该种场景下，企业的排号系统调用策略管理中心的接口自动创建访客账号并打印在排号票上。接口的调用说明请参见产品文档“北向接口”



- 访客账号管理方式:
  - 自助申请方式是指访客来访后，访问认证或注册页面，提交访客账号申请，并由接待员工或管理员审批通过，或自动审批通过。
  - 接待员工或管理员创建访客账号是指在访客来访前，接待员工或管理员先创建访客账号，访客来访后可以直接使用账号认证，无需再申请
- 访客账号管理的流程
  - 页面定制，账号申请和审批，账号创建 访客账号可以由访客自助申请，也可以由管理员或接待员工直接创建，自助申请时，访客通过访客认证页面进入注册页面，或者直接在注册页面提交申请，访客认证页面和注册页面由管理员事先定制好。定制页面时还可以配置申请的审批模式：自动审批，管理员或接待员工审批。
  - 账号分发 访客账号创建完或审批通过后，服务器在Web页面通知或发送短信、邮件通知访客。
  - 账号认证 获知账号和密码后，访客即能认证并接入网络。
  - 账号审计和管理 访客接入后，管理员可以审计访客的上下线记录，配置账号有效期并自动注销和清理过期账号。



- 本流程图是自主访客申请的配置流程，管理员审批。

访客参数设置

- 配置路径：用户与终端>访客管理>参数配置，在基本参数配置标签栏，选择启用访客注册申请，单击 选择研发部为默认访客部门，单击“确定”。

当前位置：用户与终端 > 访客管理 > 参数配置

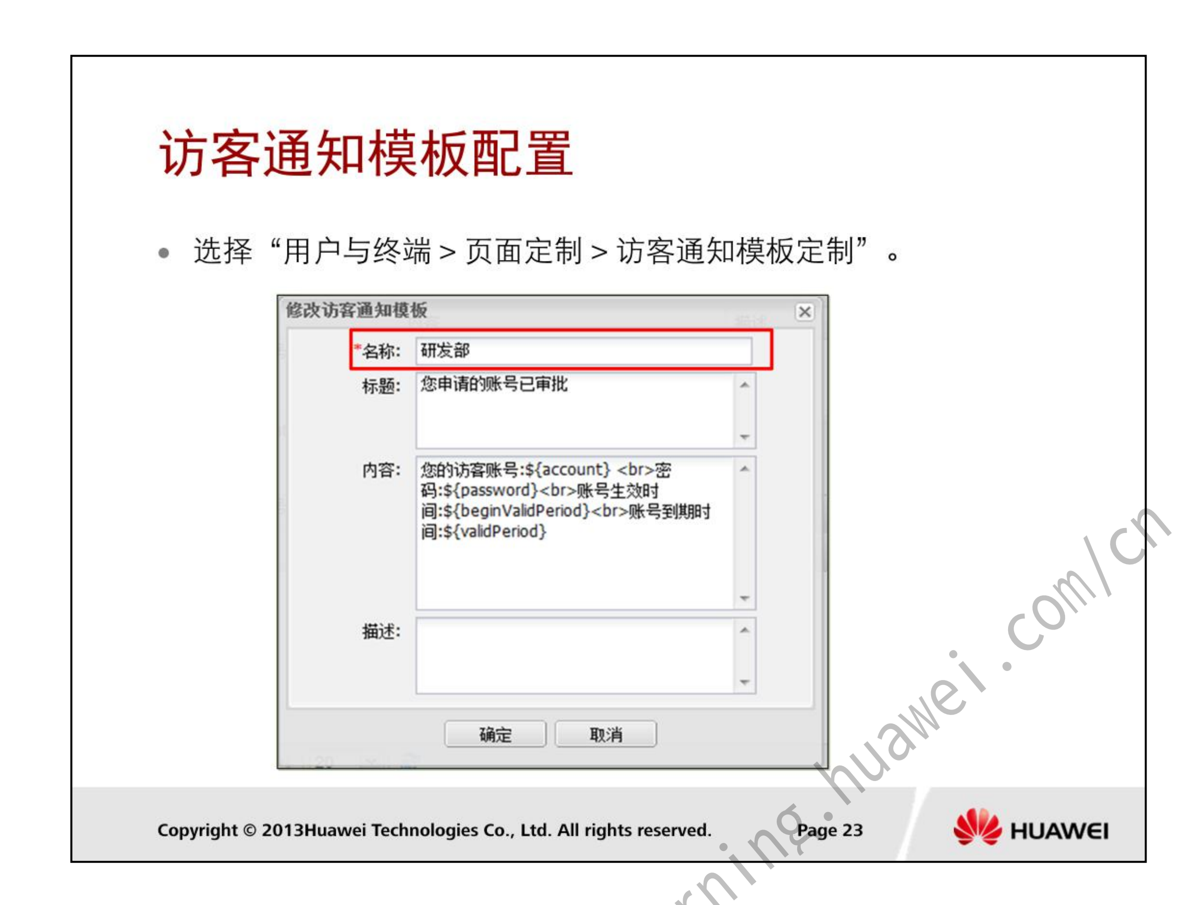
基本参数配置

访客账号申请: 启用，允许终端用户提交访客账号申请
禁用，不允许终端用户提交访客账号申请

*访客默认部门: ROOT\研发部

确定

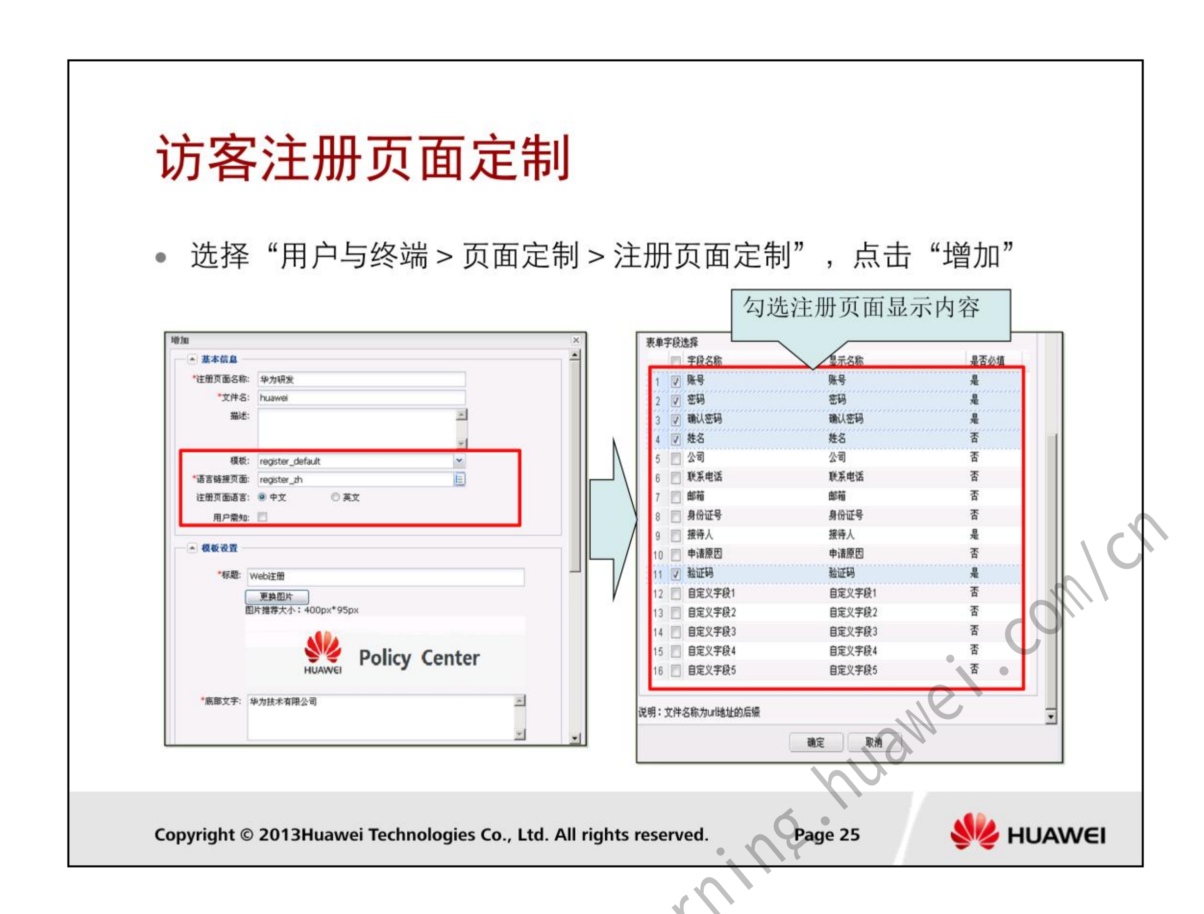
- 注意：访客管理功能默认是开启的。研发部的访客用户在身份认证和安全检查通过后能够访问研发部的网络资源。



- 访客申请的账号审批通过后，服务器按照通知模板向访客发送邮件或短信。管理员可以定制不同模板，例如，发送邮件或短信时按不同模板发送，或使用不同语种向不同用户发送。



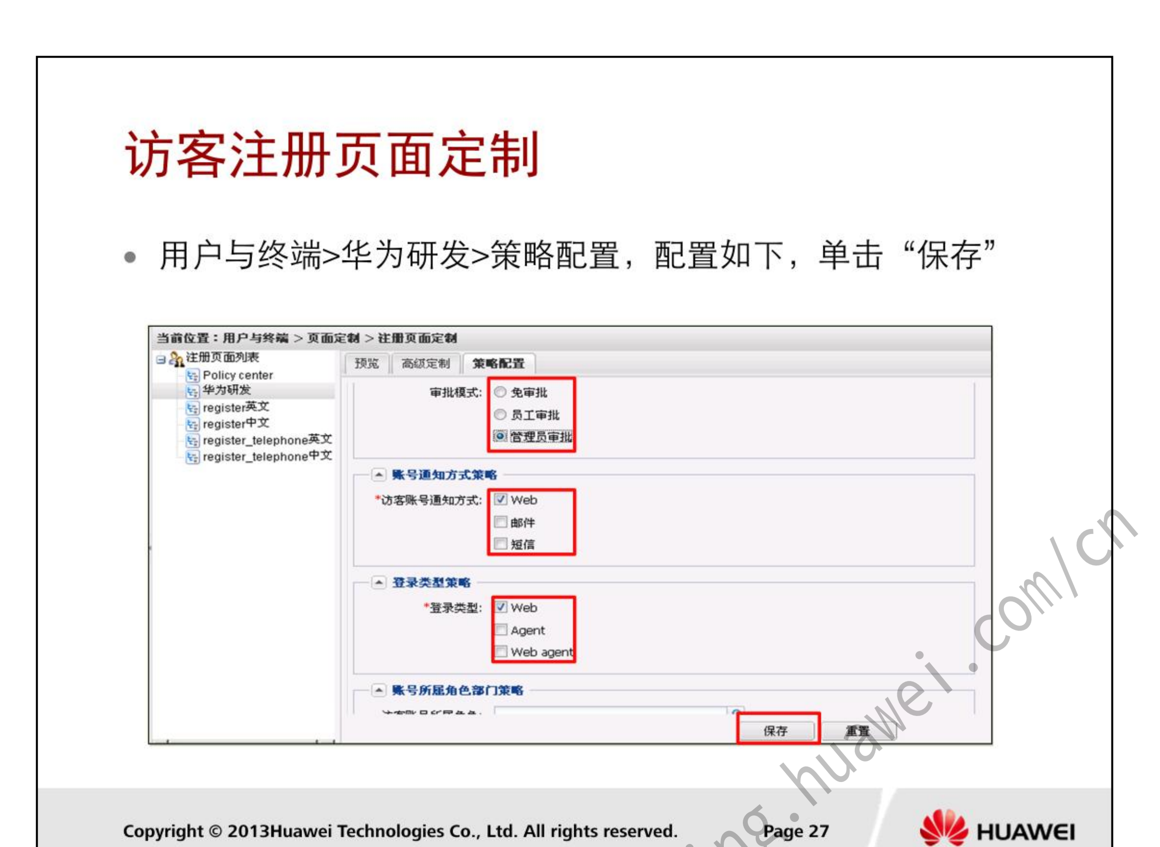
- 模板设置：可设置标题、修改认证界面图片等。



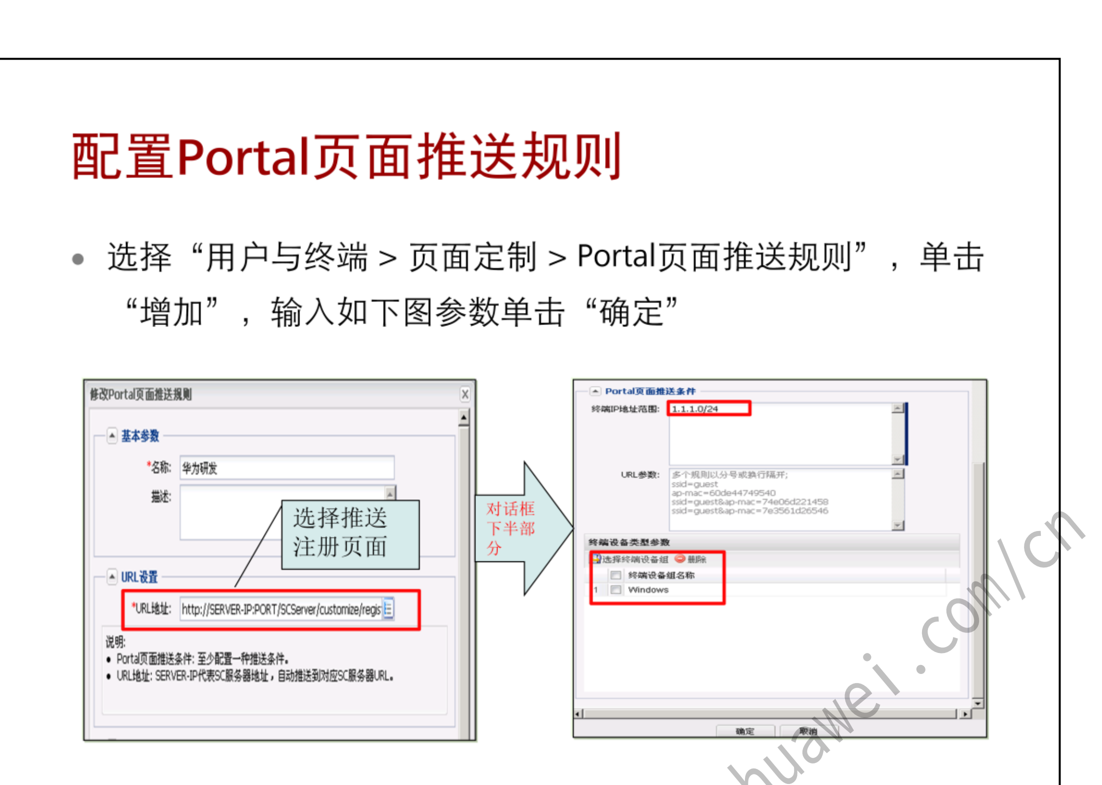
- 勾选了相应的选项，在访客注册界面将会出现该选项，如果审批方式是接待人，则接待人选项必选。



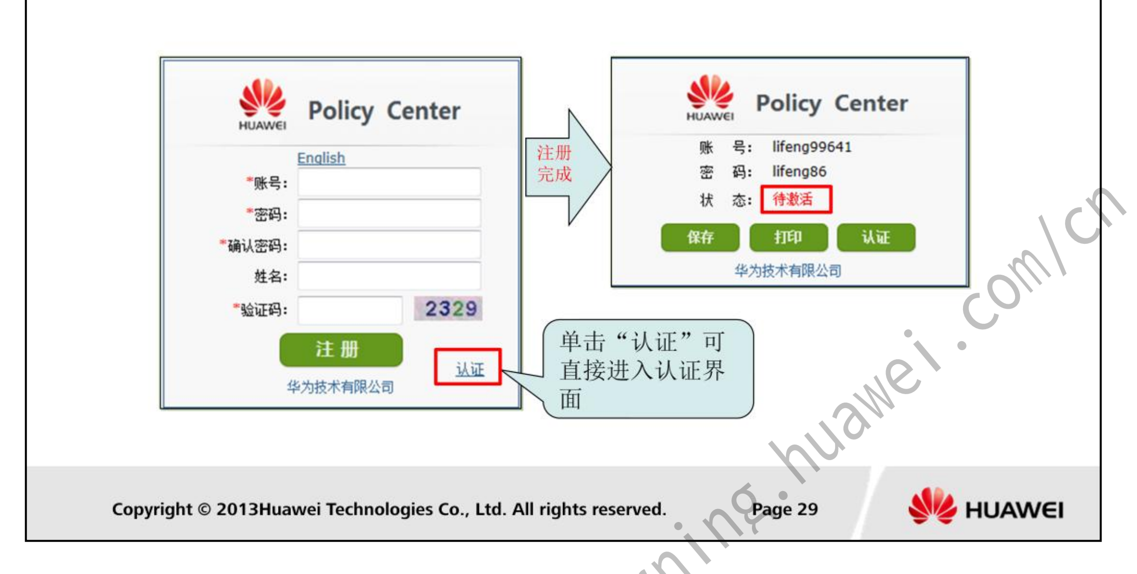
- 高级定制，则可以通过修改代码，增加自定义选项及界面，完成后需单击保存下发。



- 注意配置审批方式、访客登陆方式。



- 注意：Portal页面推送条件，必须配置一项，终端设备类型按照终端操作系统选择。



- 完成账号、密码等输入后，单击注册，出现界面显示账号及密码信息，对于访客用户建议保存账号及密码，等待审批。



- 注意：在审批建议栏输入审批建议，单击“批准”，审批通过后在访客账号管理界面，可以通过邮件、短信等通知访客审批信息。



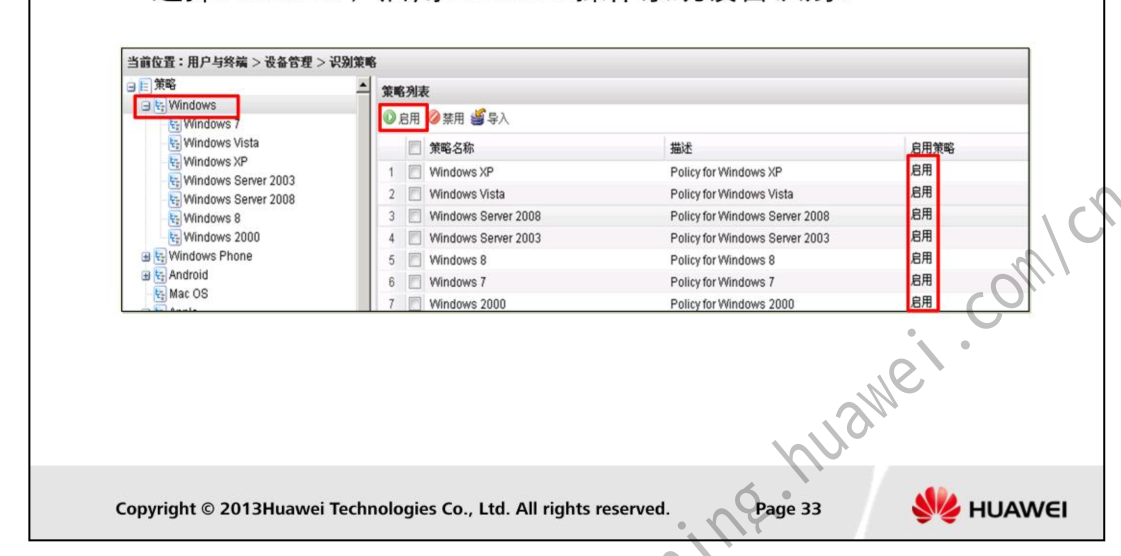
- 在IE地址栏输入http://server-ip:8080/portal，会推送出注册界面，然后单击注册按钮右下侧“认证”按钮，进入认证界面。
- 认证成功后界面不要关闭，否则需重新登陆。

设备管理-参数设置

- 配置路径：用户与终端>设备管理>参数设置，启用设备识别、手工注册、自主绑定MAC，单个用户可注册的设备数量为10。



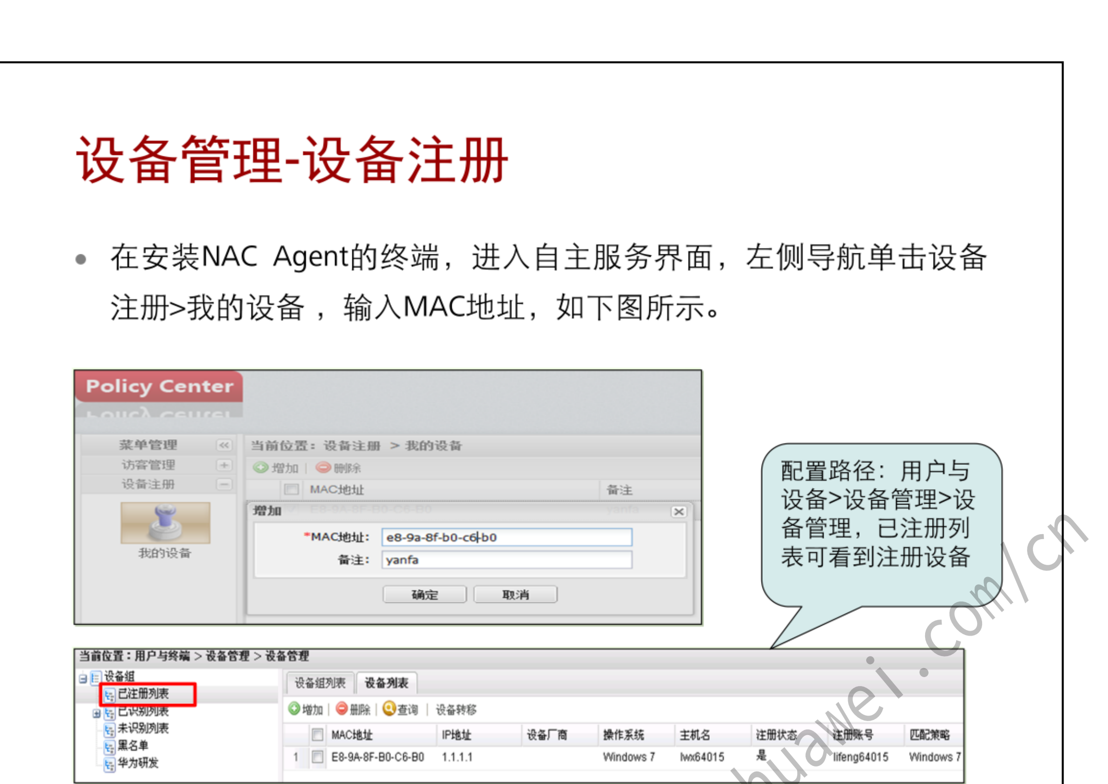
- 为了帮助管理员了解网络中存在的设备及其详细信息，管理员需要通过策略管理中心对网络进行设备探测和识别，以便管理员对设备进行分组，并按设备组进行认证和授权。
- 设备识别是网络管理最基本任务之一，通过主动查询或被动侦测来分辨将要接入网络的设备类型、IP地址、MAC地址、厂商、操作系统等设备信息，方便管理员按设备类型进行分组，并对设备进行认证和授权。
- 策略管理中心识别设备的目的是根据用户使用的终端设备类型进行授权，使不同类型的设备接入时拥有不同的网络访问权限。



- 在设备识别策略中选择相应操作系统，点击启用，本实例中启用Windows操作系统识别。



- 终端安装Win7操作系统，登陆成功后，在设备管理已识别设备中，可以看到登陆终端信息，但是注册状态是“否”。



- 注册完成后，在已注册列表中可以看到注册的主机终端信息。



目录

1. **运营管理操作**
   - 1.1 终端安全规则管理
   - 1.2 用户与终端管理
   - 1.3 软件分发管理
   - 1.4 资产管理
   - 1.5 补丁管理
   - 1.6 USB管理
2. **系统维护**
3. **运维工具**



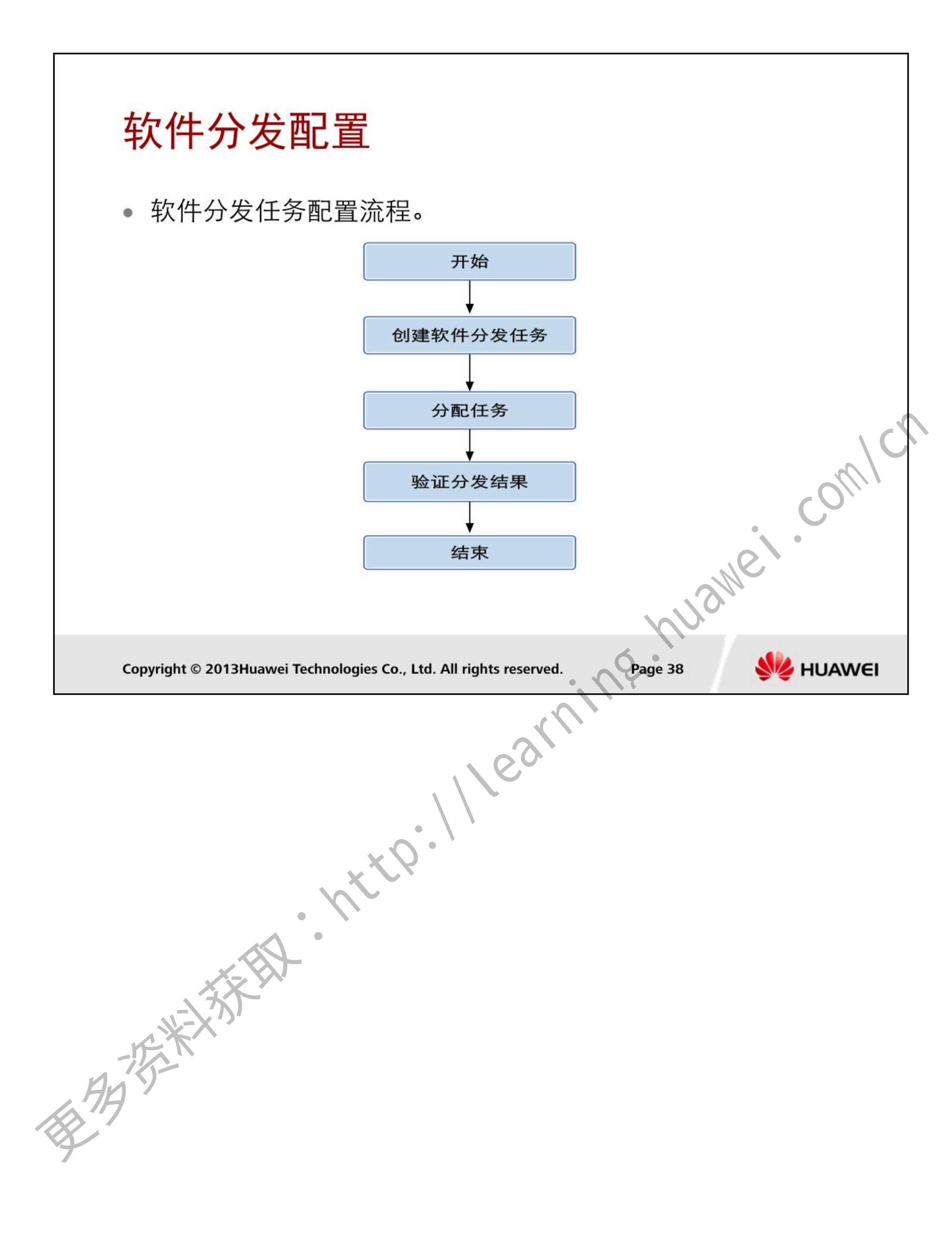
- 本节主要介绍终端安全系统软件分发功能。

软件分发

- 软件分发是指管理员利用NAC Agent将软件从安全管理器自动下载至终端主机，并且在终端主机自动运行或安装的过程



- 所谓软件分发是指管理员利用NAC Agent将软件从安全管理器自动下载至终端主机，并且在终端主机自动运行或安装的过程。
- 软件分发解决如何协助管理员在若干个部门的终端主机下发软件并且自动安装软件的问题。通过向软件提供静默安装参数，NAC Agent能够在不影响终端用户正常办公的情况下在终端主机安装，有效缓解软件在组织范围内推广困难的问题，并且降低IT运维成本。
- 安全管理器只支持以NAC Agent的方式接入受控网络的终端主机进行软件下载和自动安装，不支持Web Agent插件和Web客户端方式接入受控网络的终端主机进行软件下载和自动安


软件分发配置
软件分发任务配置流程。
开始
创建软件分发任务
分配任务
验证分发结果
结束
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 38
HUAWEI

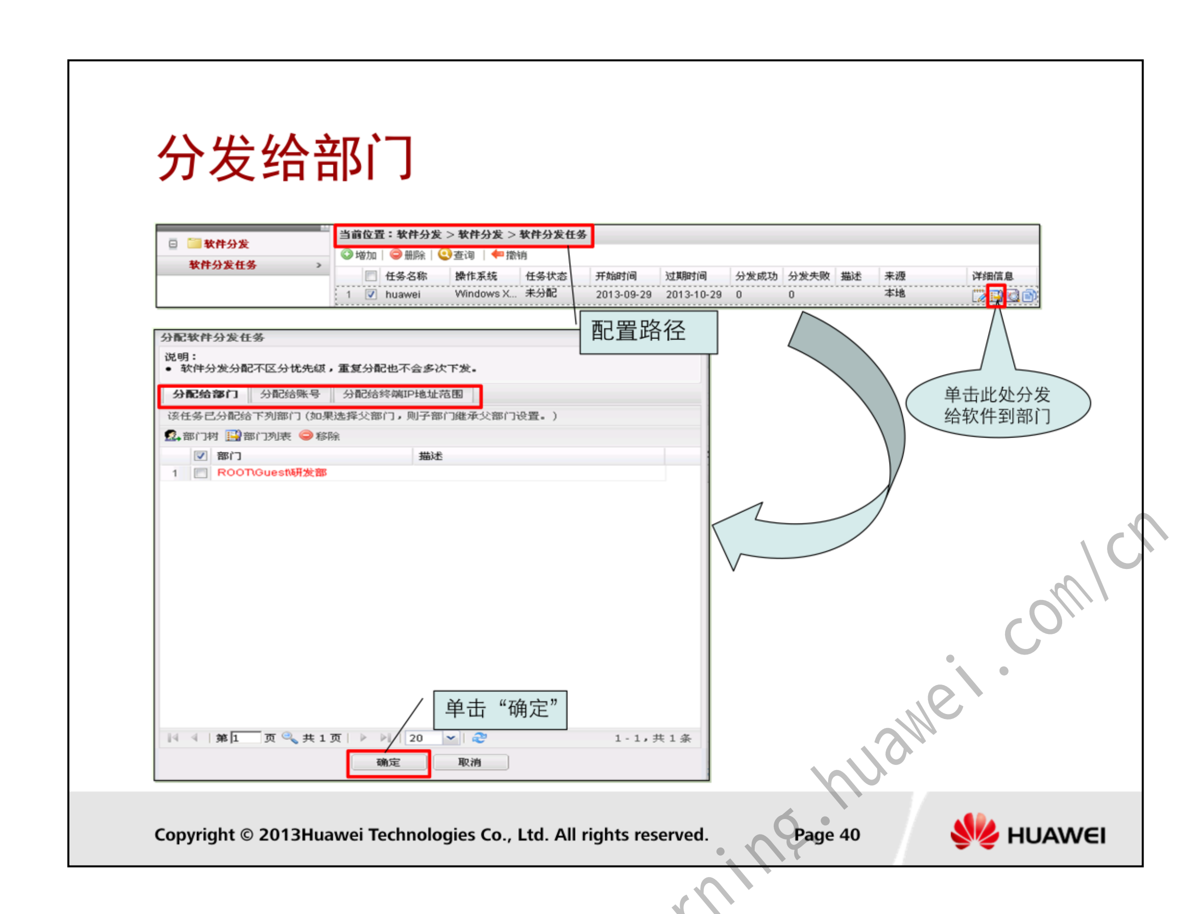
通过内部数据源分发软件

- 选择“软件分发 > 软件分发 > 软件分发任务”。
- 单击“增加”，配置完成后单击“确定”

举例：分发搜狗输入法

HUAWEI

- 所谓内部数据源是指待分发的软件来自Policy Center的源FTP服务器或镜像FTP服务器。
- 从内部数据源下载软件并且当软件分发任务执行成功时，Anget代理将会获取待分发的软件，而不是待分发软件在源FTP服务器或镜像FTP服务器的路径。通过内部数据源分发软件，操作比较灵活，传输速率比较快，软件分发到终端后提供自动执行可执行文件的功能。
- 所谓外部数据源是指待分发的软件来自Policy Center的源FTP服务器或镜像FTP服务器以外的文件服务器。
- 在分发软件时管理器只会把待分发软件在外部数据源的路径发送给Agent代理，终端用户在代理看到待分发软件的路径，单击超级链接即可下载。外部数据源能够分发如下类型的文件服务器的文件：
  - HTTP服务器
  - FTP服务器
  - Microsoft Windows文件共享服务器
- 通过外部数据源分发软件，只支持分发一个链接，不直接下载软件。终端用户需要通过手工的方式，点击下载链接下载软件。由于不能直接下载软件，选择分发外部文件服务器中的软件时，不提供自动执行可执行文件的功能。



- 通过为部门分配软件分发任务，可将任务分发至某个部门的所有终端，当分发条件满足时，开始执行分发任务。



- 研发部在线终端将收到所分发的软件。



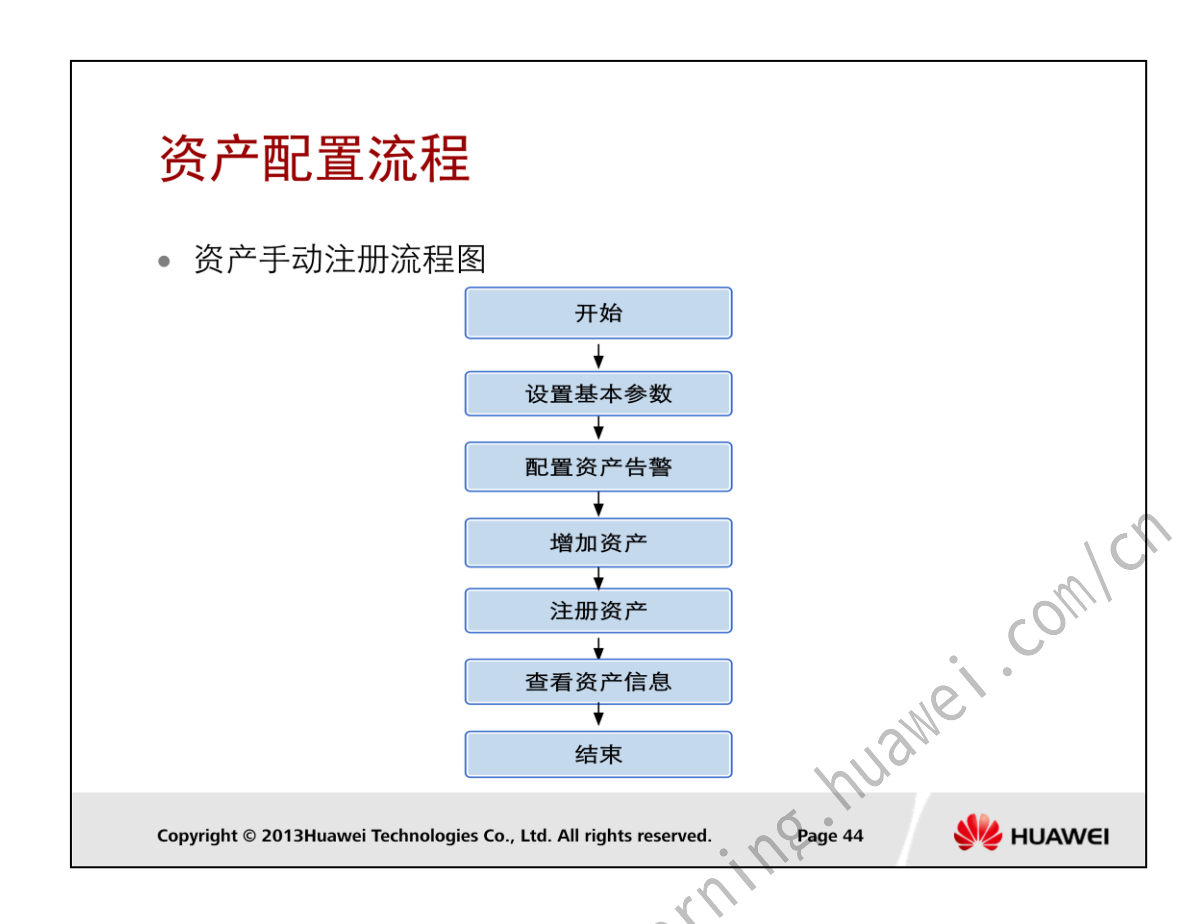
目录



- 本节主要介绍终端安全系统资产管理配置



- 资产管理相关概念：
  - 游离资产指没有设定资产责任人的资产如果管理员没有为资产设定资产责任人，或者所设定的资产人账号已被删除，则资产会变为游离资产。
  - 自动注册资产是指由Policy Center管理器自动为终端主机分配一个唯一的资产编号管理员在设置自动注册资产后，当代理首次连接Policy Center控制器成功时，将收到Policy Center管理器分配的唯一的资产编号。通过资产编号能够帮助管理员快速检索终端主机的软硬件资产信息。
  - 所谓手工注册资产是指由管理员通过手工方式在Policy Center管理器创建一条资产记录，并将资产编号分配给终端用户，终端用户在代理输入资产编号完成资产注册过程。
  - 所谓资产变更是指在终端主机安装或卸载软件，安装或拆卸硬件部件引起的终端主机的软硬件信息变更。当资产发生变更时，代理将会把资产变更信息上报给Policy Center管理器，管理员通过查询变更报表即可获取近期有哪些资产发生过变更，提醒资产责任人及时了解软件的安装卸载情况。
  - 所谓软件许可管理是指通过代理统计使用指定软件的终端用户数量，管理员通过统计终端用户正在使用软件的数量，了解指定软件的使用情况，方便管理员对安装的软件进行有效的管理和维护。



- 注意：按照本流程图配置完成后，要查看资产告警，可以去系统维护模块儿查看资产告警信息。



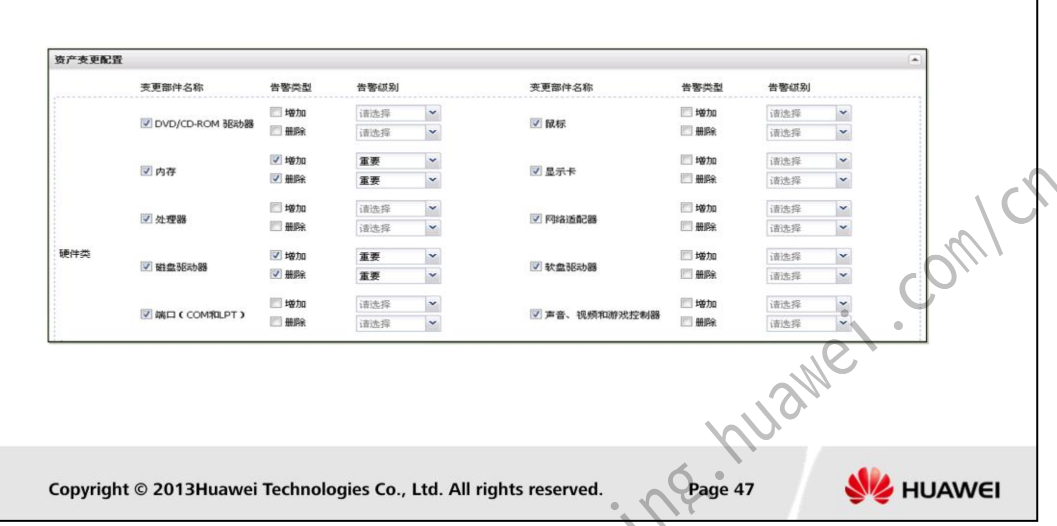
- 资产注册模式包括自动注册和手工注册。自动注册模式不需要终端用户参与，自动完成资产的注册。手动注册需要终端用户在NAC Agent代理手工进行资产注册操作。



- 通过配置资产信息的上报参数，管理员能够设置需要上报的资产信息类别。

设置资产变更的上报参数

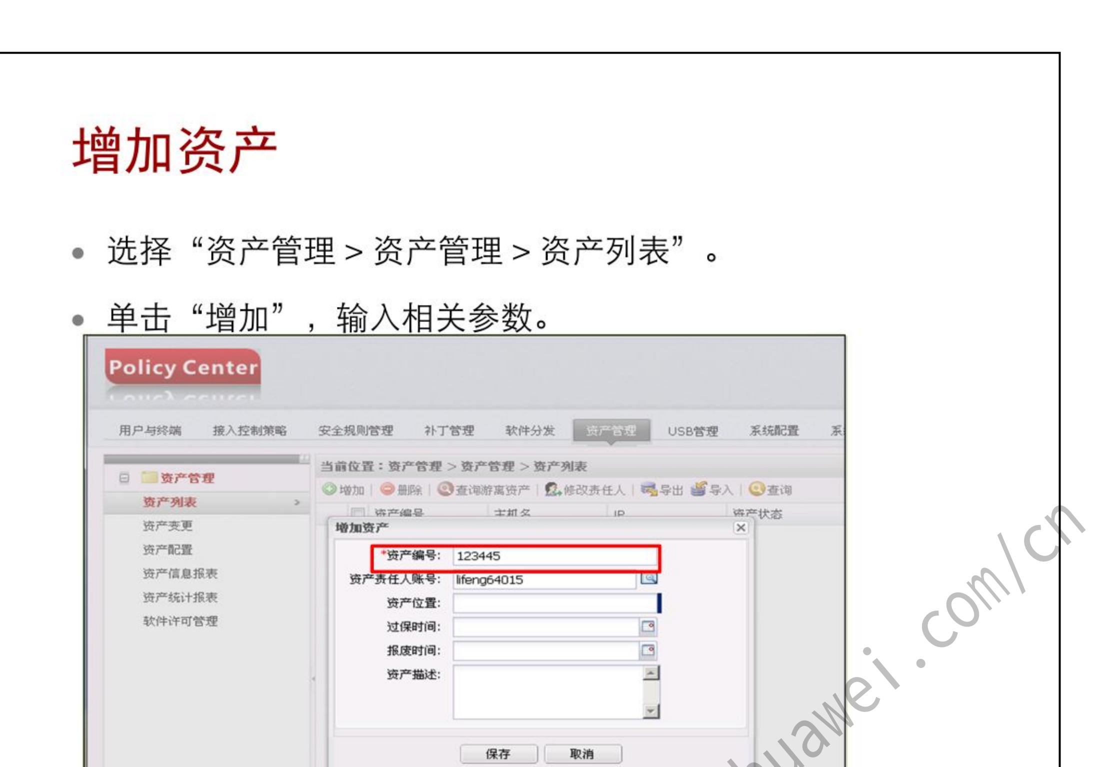
- 选择“资产管理 > 资产管理 > 资产配置”。
- 在“资产变更配置”区域框中设置配置参数。



- 通过配置资产变更的上报参数，管理员可以根据资产变更类型及重要程度设置资产信息发生变更后是否上报。



- 通过配置资产变更告警邮件，可以及时将资产告警信息发送给相关人员。



- 为了便于管理器集中管理和维护企业中的所有资产信息，当新设备开始投入使用时，管理员需要将资产信息录入管理器。本操作适用于增加少量（小于或等于3台）资产信息。
- 管理员在增加资产信息时，能够为资产设定责任人和资产位置。当资产所在的位置发生变更时，终端用户能够在代理设置资产的位置，以便更新资产位置信息。
- 当资产责任人账号被删除后，资产与该资产责任人的归属关系自动解除，即资产的“资产责任人账号”属性被自动清空，该资产成为游离资产。



- 资产注册，资产编号：123445.



- 资产注册成功后，NAC Agent代理将立即上报终端主机的软件和硬件信息。上报成功后，管理员能够查看已注册终端主机的软件和硬件信息。



- 资产信息报表为管理员提供该资产最新最详尽的信息，包括资产编码、所在部门、责任负责人等。



- 通过查询资产的统计报表，管理员可以通过部门、操作系统、资产状态等信息查看资产的统计情况。





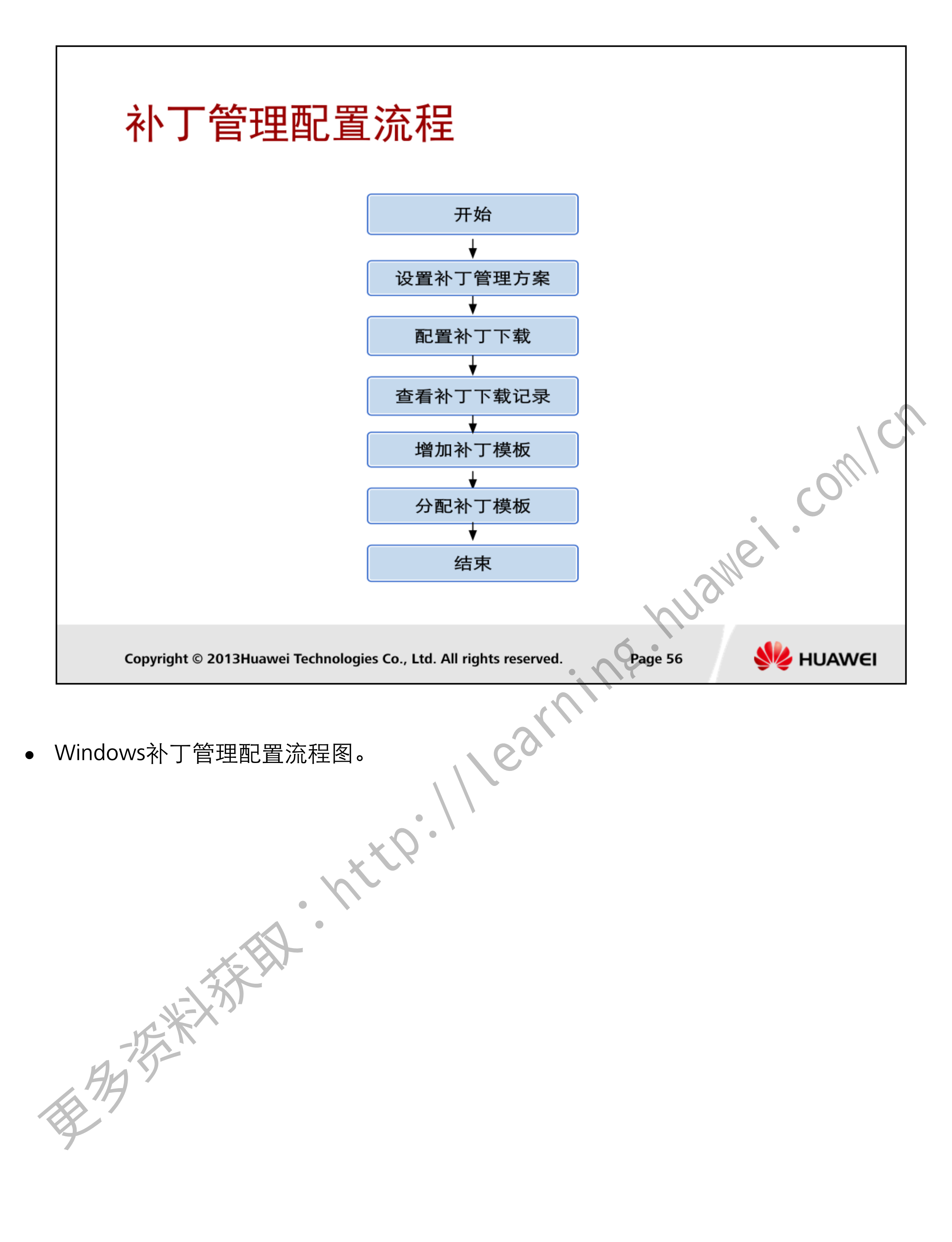
- 本节主要介绍终端安全系统补丁管理配置。

补丁管理

- 通过补丁管理功能Policy Center管理器为终端主机安装Microsoft Windows或Linux操作系统的补丁。



- 操作系统给终端用户带来便捷的同时，由于终端用户对安装操作系统补丁不重视，已发现的操作系统安全漏洞无法得到及时修复，导致终端主机容易感染病毒或木马，成为网络安全的薄弱环节。如何确保操作系统的安全是管理员最关注的焦点之一。
- 较好的解决办法是通过工具协助终端用户自动安装操作系统补丁，及时封堵安全漏洞，最大限度降低病毒或木马利用操作系统的漏洞进行传播、盗取机密信息或进行破坏
- Policy Center支持对Windows和Linux操作系统的补丁管理。

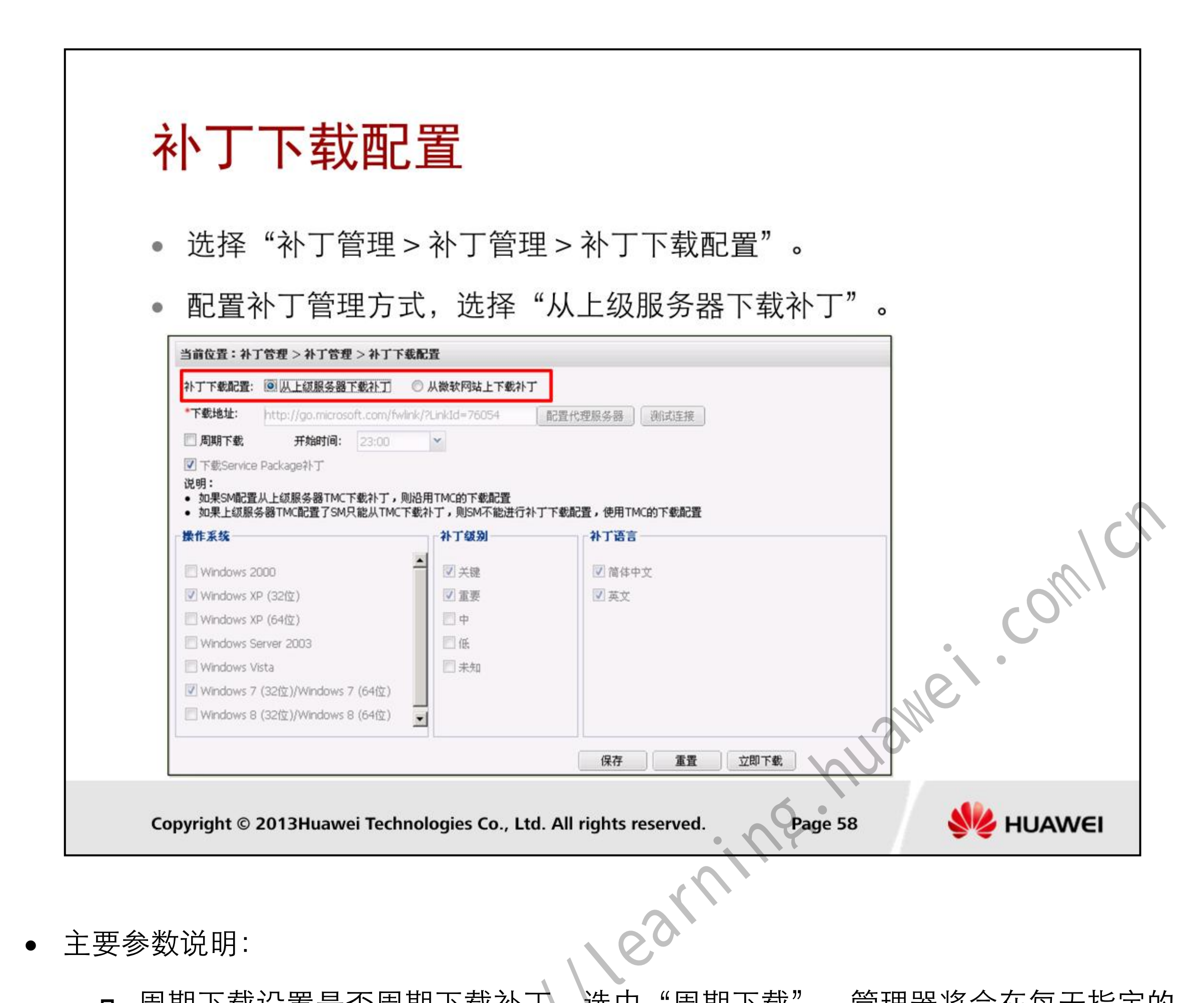


- Windows补丁管理配置流程图。

设置补丁管理方案

- 选择“补丁管理 > 补丁管理方式 > 补丁管理方式”。

- 补丁管理方案包括以下三种：使用Policy Center系统自有的补丁下载和分发功能，使用微软WSUS系统的补丁下载和分发功能，不提供补丁下载和分发功能。
- 管理器与WSUS联动适用于在安装Policy Center之前已经安装WSUS的场合。管理器与WSUS不仅能协助终端用户安装Microsoft Windows操作系统补丁，还能在终端主机未安装补丁的情况下禁止终端主机接入受控网络。
- Microsoft Windows补丁管理与Microsoft Windows补丁检查策略均能检查终端主机是否已经安装指定的Microsoft Windows操作系统补丁，不同点在于：
  - Microsoft Windows补丁检查策略重在检查终端主机是否安装Microsoft Windows操作系统的补丁，并且能够与检查结果对终端主机进行接入控制。当终端主机未安装指定的Microsoft Windows操作系统补丁时禁止终端主机接入受控网络，而不是协助终端用户自动安装Microsoft Windows补丁。在这种情况下，管理员必须配置Microsoft Windows补丁检查策略与Microsoft Windows补丁管理联动，或者与WSUS联动才能实现自动安装Microsoft Windows补丁，否则，终端用户只能手工下载并安装补丁才能消除违规。
  - Microsoft Windows补丁管理重在检查终端主机是否安装指定的补丁，根据SM管理器配置的Microsoft Windows补丁部署规则协助终端主机下载并安装指定的补丁，而不是对终端主机进行接入控制。



- 主要参数说明：
  - 周期下载设置是否周期下载补丁。选中“周期下载”，管理器将会在每天指定的时间开始下载新增的补丁。如果不选中“周期下载”。
  - 开始时间，当选择“周期下载”时为必填项设置SM管理器下载补丁的开始时间，仅支持整点开始执行下载任务。建议设为业务空闲期，例如“0:00”。



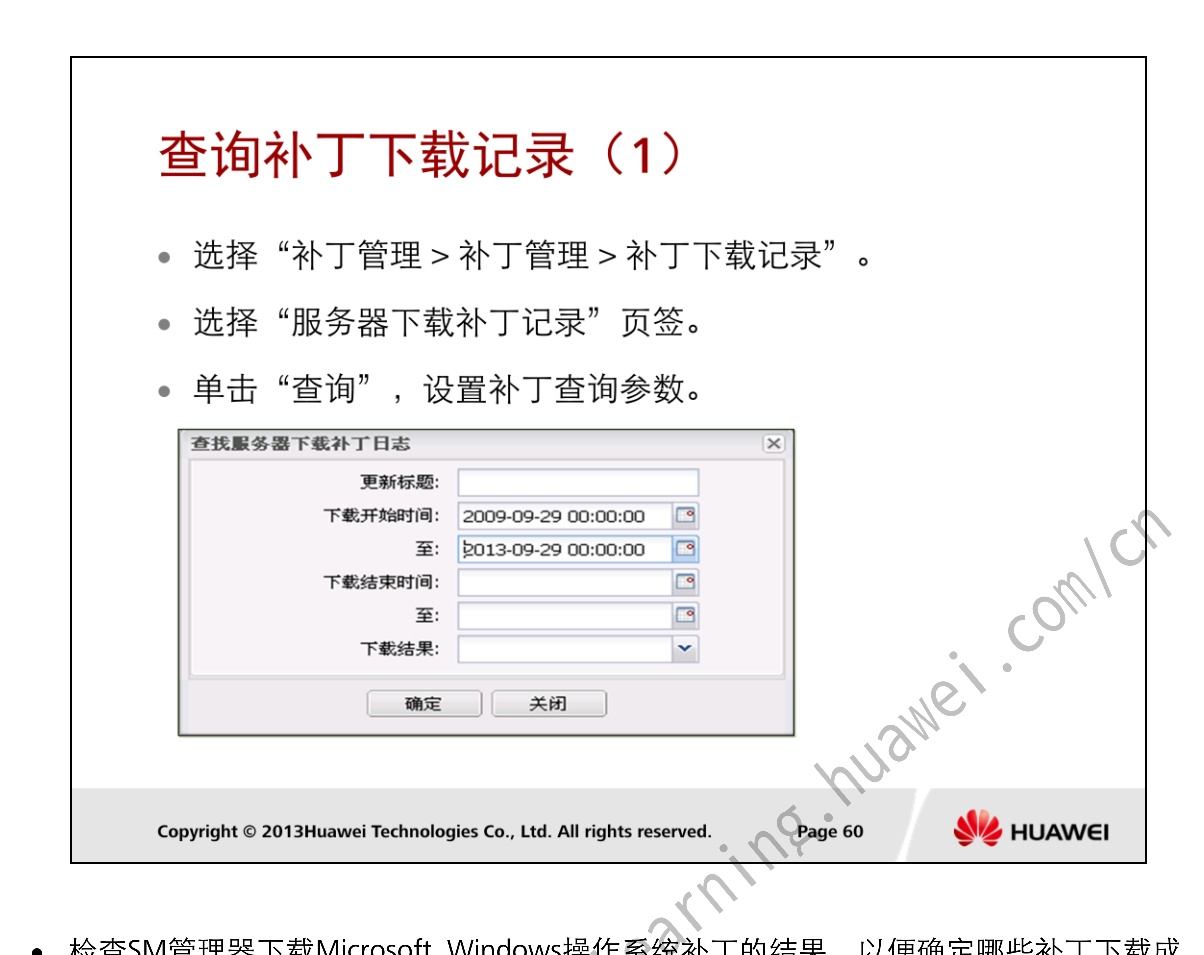
查询补丁下载记录

- 选择“补丁管理 > 补丁管理 > 补丁下载记录”。
- 选择“服务器特征库下载记录”页签。



	下载开始时间	下载结束时间	文件大小(KB)	特征库版本	特征库发布时间	下载结果	失败原因	重试次数
1	2009-11-28 20:19:54	2009-11-28 20:20:47	17349.924	5.8.0.2678	2009-11-09 23:15:59	下载成功	无	0

- 查询补丁特征库的下载结果，以便了解补丁特征库是否得到及时更新。
- 补丁特征库是否得到及时更新将影响到SM管理器下载Microsoft Windows操作系统补丁的效果。如果补丁特征库没有得到及时更新，将会导致SM管理器无法从微软官方网站下载新增的补丁。如果SM管理器无法下载Microsoft Windows补丁，请检查补丁特征库下载失败。



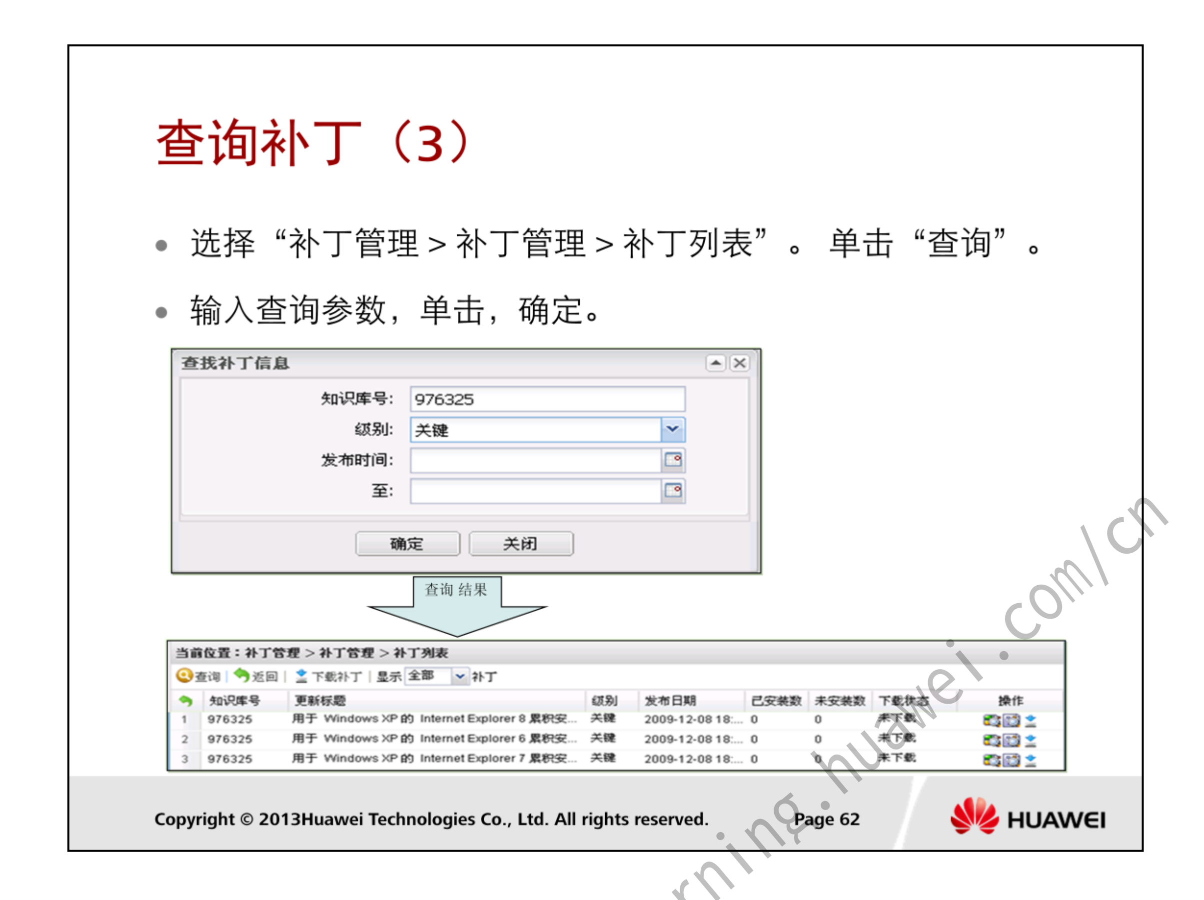
- 检查SM管理器下载Microsoft Windows操作系统补丁的结果，以便确定哪些补丁下载成功，哪些补丁下载失败。

查询补丁下载记录（2）

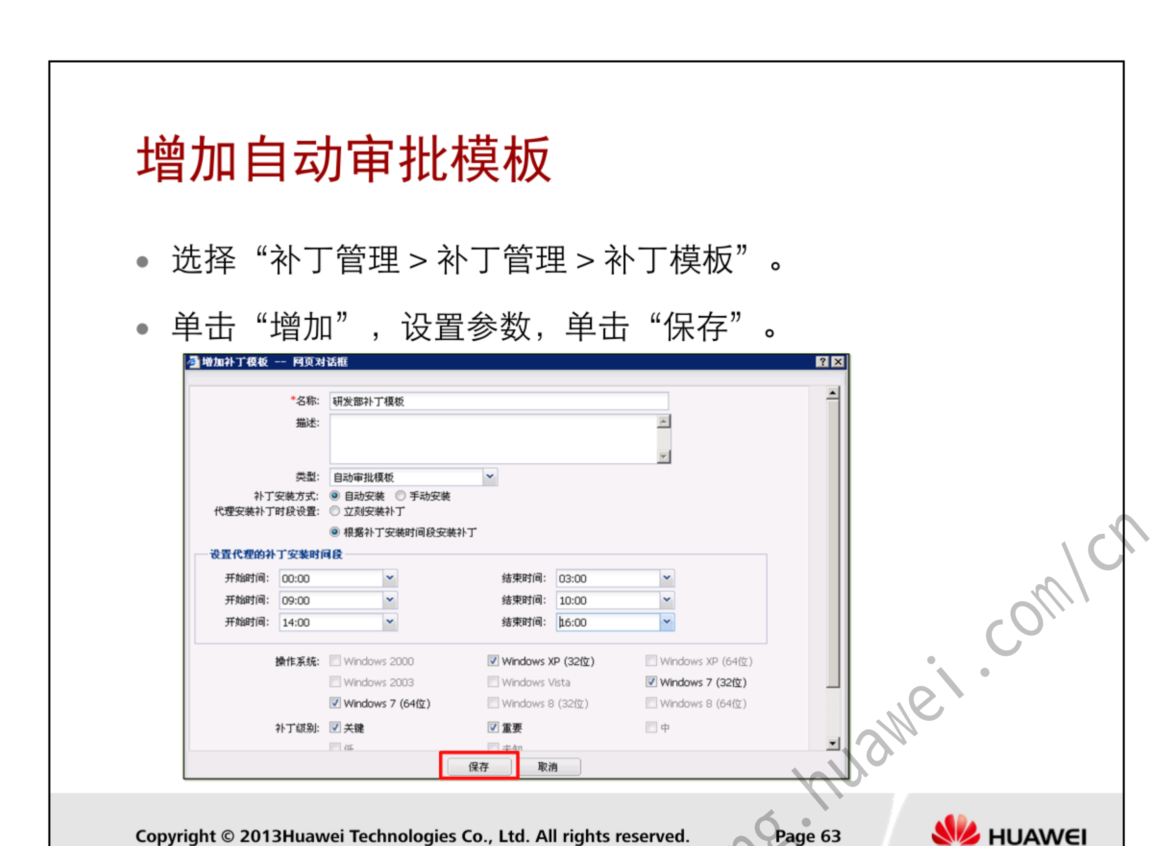
- 单击 查看补丁下载日志的详细信息。

知识库号	2229593
更新标题	Windows XP 安全更新程序（KB2229593）
下载开始时间	2012-01-05 23:12:22
下载结束时间	2012-01-05 23:12:25
发布日期	2010-07-06 21:58:41
下载结果	成功
重试次数	0
失败原因	
级别	关键
描述	现已确认有一个安全问题，未通过身份验证的远程攻击者可能会利用此问题危及系统的安全并获取对该系统的控制权。您可以通过安装本 Microsoft 更新程序来保护系统不受侵害。安装本更新程序后，可能必须重新启动系统。
公告号	MS10-042
适用语言	葡萄牙语
更多信息	http://go.microsoft.com/fwlink/?LinkId=194729
官方URL地址	http://download.windowsupdate.com/msdownload/update/software/secu/2010/06/windowsxp-kb2229593-x86-ptg_62c4cce5e7f9f666d025422feaebe51b66b0aa17.exe

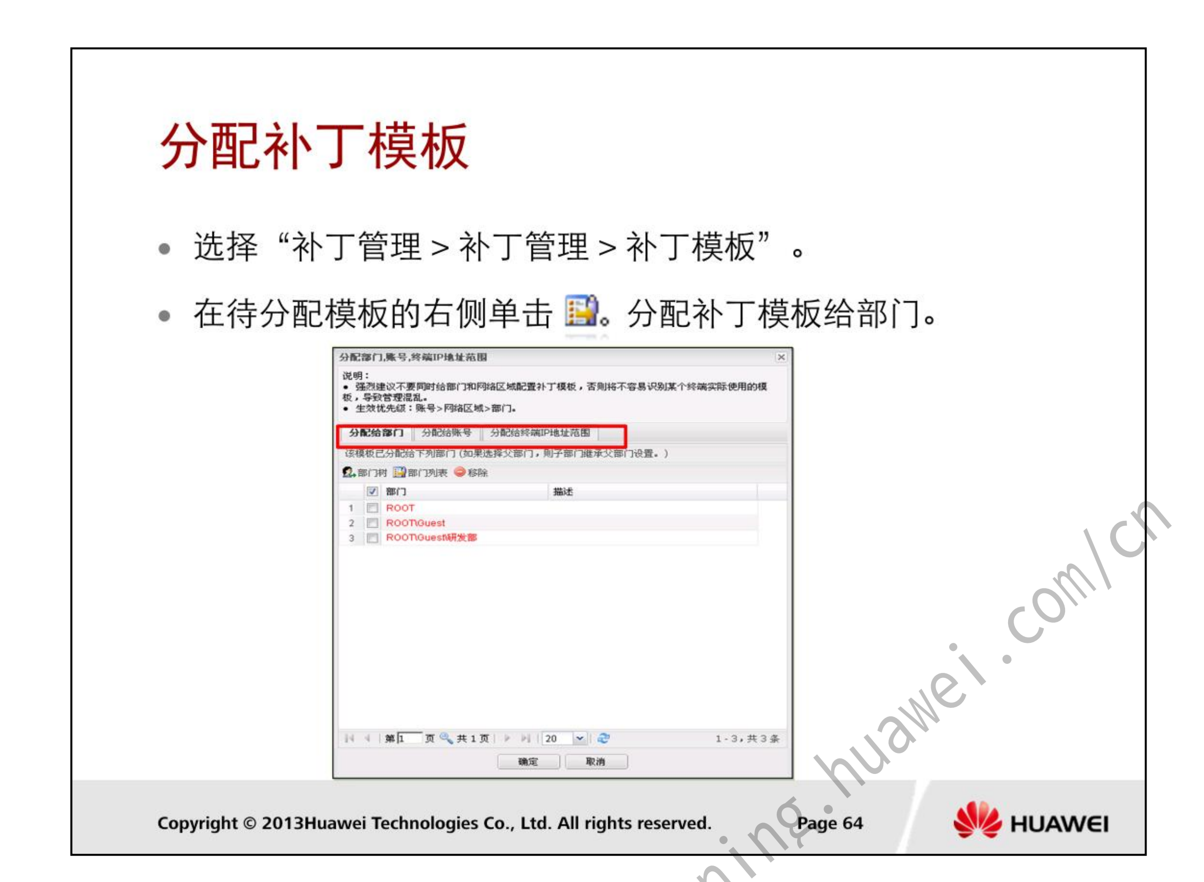




- 查询补丁，以便管理员了解当前管理器存储哪些补丁，或方便管理员查询指定补丁的相关信息和安装情况。



- 创建自动审批补丁模板，匹配设置条件匹配需要安装的补丁，以便通知终端主机从管理器下载和安装需要的Microsoft Windows操作系统补丁。
- 自动审批补丁模板适用于为终端用户设置条件匹配需要安装的Microsoft Windows操作系统补丁场合，不匹配的补丁则不会在终端主机安装，而无需管理员逐一挑选需要安装的补丁。



- 补丁模板可以指派给部门、账号和网络安全区域。如果不同的补丁模板分别应用到部门、账号和网络区域，则优先级最高者所分配到的补丁模板将会生效。部门、账号、网络区域的优先级关系为：账号 > 网络区域 > 部门。
- 当同时为部门和网络区域分配补丁模板时，管理员要判定某个员工使用了什么模板，不仅要考虑员工在哪个部门，还要考虑该员工在哪个网络区域的终端主机上进行认证。当员工在不同网络区域认证时，各个网络区域配置的补丁模板不一样，员工使用的模板也就不一样。这就增加了管理员管理的复杂度。因此，建议管理员不要同时为部门和网络区域分配补丁模板。



目录



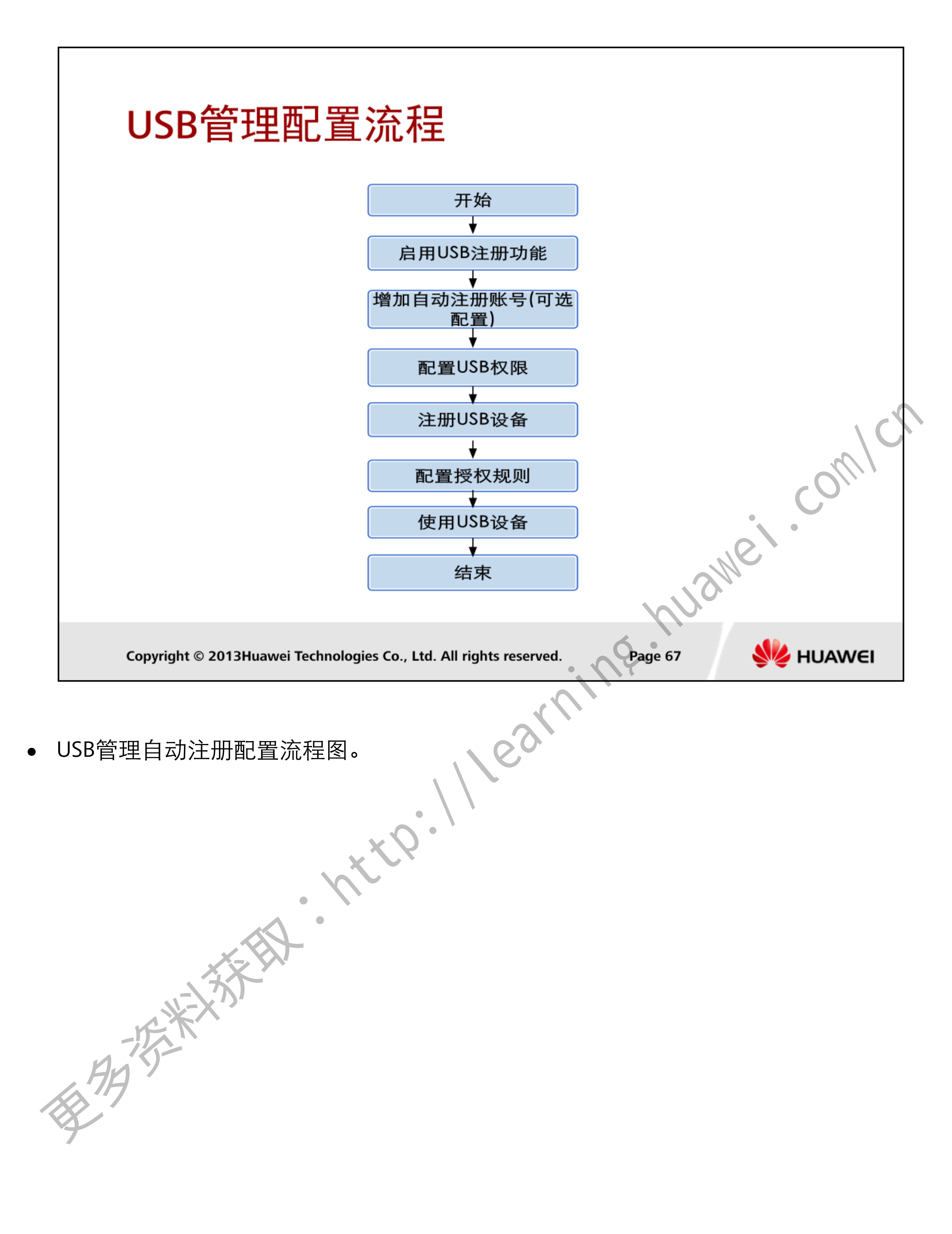
- 本节主要介绍终端安全系统USB管理

USB管理

- USB存储设备的管理包括USB存储设备的注册和审批、解除注册、使用权限、使用范围限制、挂失和解除挂失、离线解密，以及USB存储设备的规格说明。



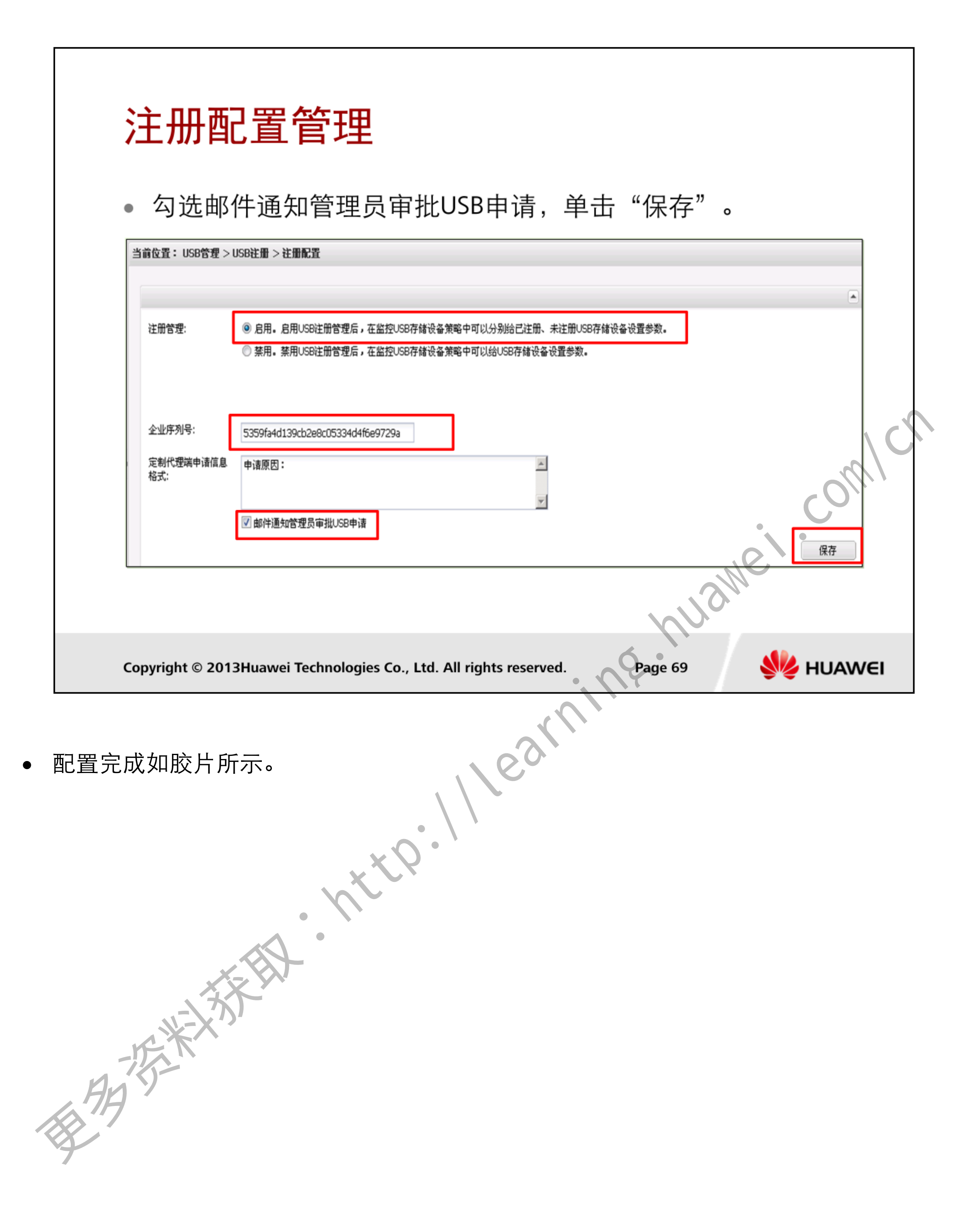
- USB存储设备管理功能通过注册USB存储设备，能够管理企业内部的USB存储设备。
- 企业员工对已注册和未注册的USB存储设备具有不同的使用权限。USB存储设备管理功能通过监控USB存储设备策略，实现对已注册和未注册的USB存储设备使用权限的控制。
- 由于在企业内部使用未注册的USB存储设备会受到限制，员工在使用USB存储设备前，需要通过NAC Agent代理提交注册申请。根据员工提交注册申请所使用的账号是否具有自动审批权限，所提交的注册申请的审批过程有所不同：
  - 如果提交注册申请的员工具有自动审批权限，则该注册申请自动审批通过，无需管理员审批。
  - 如果提交注册申请的员工不具有自动审批权限，则该申请提交到管理员处等待审批，管理员审核员工提交的申请，当申请属实时批准申请，当申请不属实或注册申请填写错误时拒绝申请。
- 审批通过后的USB存储设备即成为已注册的USB存储设备，当已注册的USB存储设备丢失时，管理员能够挂失丢失的USB存储设备，已挂失的USB存储设备不能使用。当挂失的USB存储设备被找回后，管理员能够解除挂失，USB存储设备能够恢复正常使用。



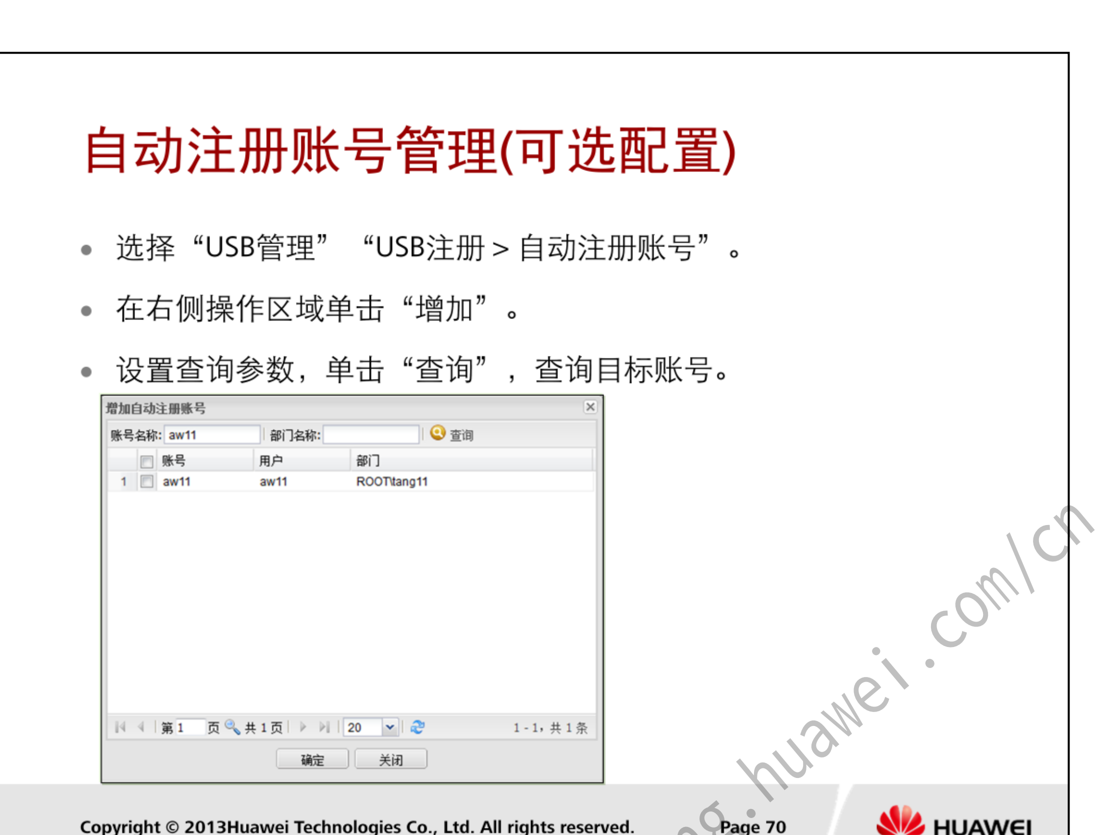
- USB管理自动注册配置流程图。



- 系统默认禁用USB存储设备注册管理功能。当需要使用USB存储设备注册管理功能时，请先执行启用USB存储设备注册管理操作。
- 企业序列号是区分各个企业的依据（即限制在本企业注册的USB存储设备只能在本企业内使用），请根据USB存储设备注册管理功能的使用情况，选择企业序列号的生成方式。
  - 自动生成，首次启用USB存储设备注册管理功能时使用。
  - 手工输入，如果Policy Center系统中的企业序列号丢失时使用。


注册配置管理
勾选邮件通知管理员审批USB申请，单击“保存”。
当前位置：USB管理 > USB注册 > 注册配置
注册管理:
启用。启用USB注册管理后，在监控USB存储设备策略中可以分别给已注册、未注册USB存储设备设置参数。
禁用。禁用USB注册管理后，在监控USB存储设备策略中可以给USB存储设备设置参数。
企业序列号:
5359fa4d139cb2e8c05334d4f6e9729a
定制代理端申请信息格式:
申请原因：
邮件通知管理员审批USB申请
保存
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 69
HUAWEI

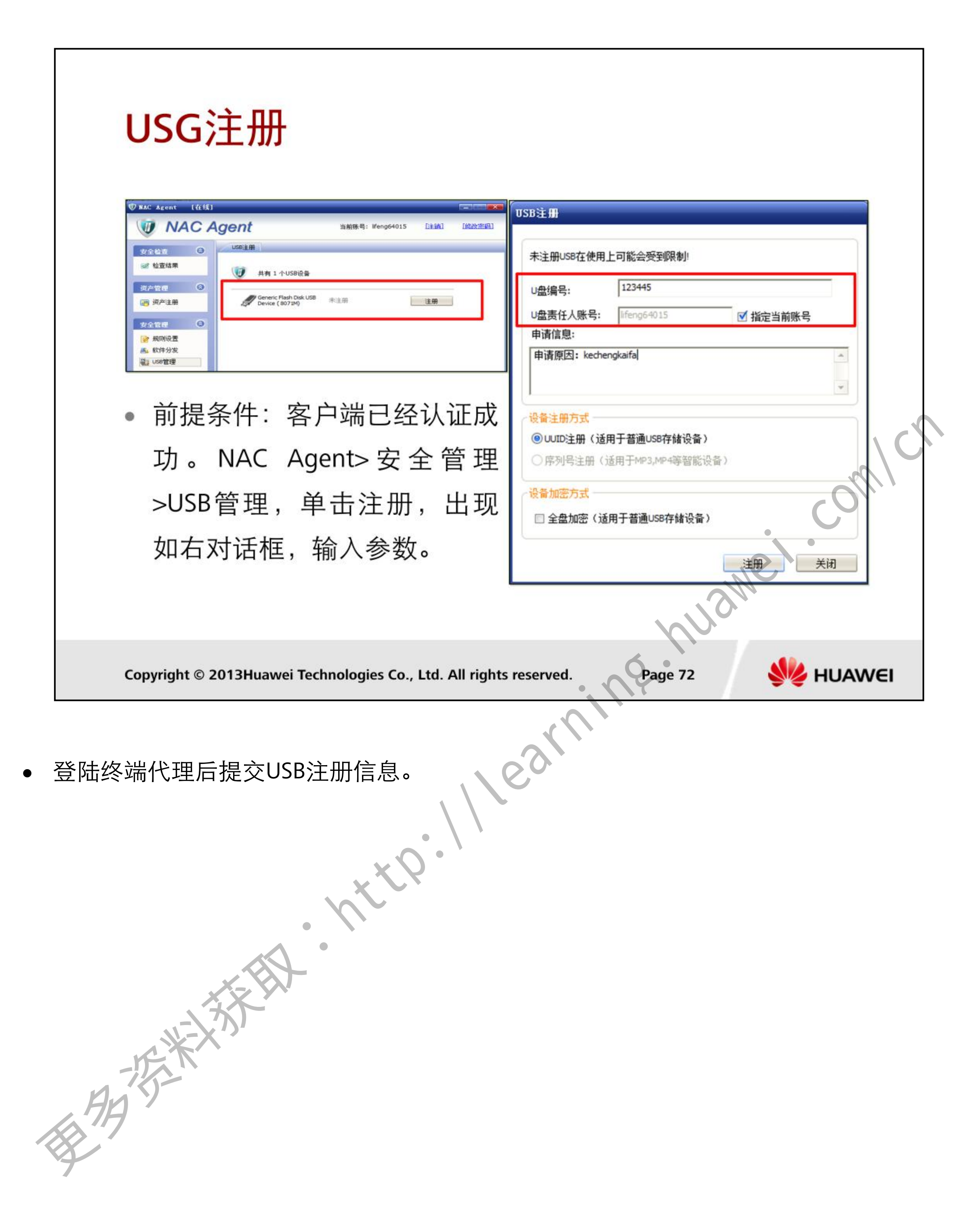
- 配置完成如胶片所示。



- 增加自动注册账号，减轻管理员审批USB存储设备注册申请的工作量，保证终端用户能够及时完成USB存储设备注册。在增加自动注册账号前，请管理员仔细审核待增加账号是否有权限自动注册USB存储设备。
- 被添加为自动注册账号后，该账号提交的注册申请能够自动审批通过，无需管理员批准。



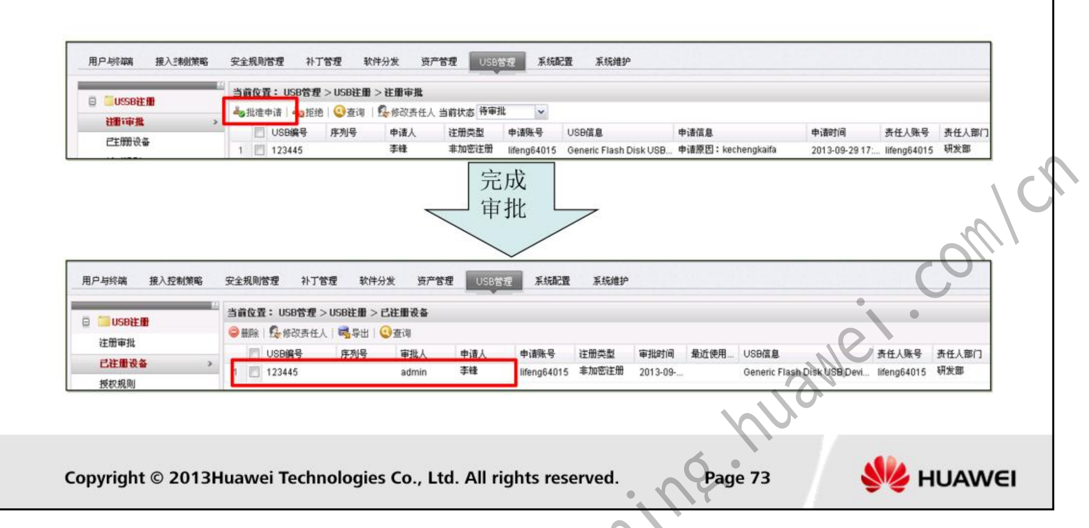
- 根据配置任务，需要为研发部内已注册和未注册的USB存储设备分别配置文件监控和禁用权限。



- 登陆终端代理后提交USB注册信息。



- USB管理>USB注册，选中待审批项，单击“批准申请”在已注册设备，可以查看到注册的设备。



HUAWEI

- 根据配置任务，员工提交的注册申请属实，管理员批准注册申请。



- 对于某些重要的USB存储设备，在注册完成后，管理员能够限定这些设备只能由指定人员使用（包括指定账号和指定部门的人员），或者只能在指定类型指定IP地址的终端上使用，避免其他人员从这些设备中获取重要信息。如果管理员没有配置设备的授权规则，则所有人都能使用该设备。

已注册设备管理

- 对于已经注册的USB存储设备，管理员能够查看已注册设备在最近30天的违规信息，进行挂失和解除挂失等操作。
- 选择“USB管理 > USB注册 > 已注册设备”，管理已注册设备:
  - 查看已注册设备的使用信息
  - 挂失已注册的USB存储设备
  - 解除挂失已注册的USB存储设备



- 查看已注册设备在最近30天的违规信息，帮助管理员了解已注册USB存储设备的违规使用信息。
- 当已经注册的USB存储设备丢失后，建议管理员及时挂失，避免由于非法使用该USB存储设备而导致泄密。
- 对于已注册的USB存储设备，管理员能够导出已注册设备列表，并查询和删除已注册的USB存储设备。





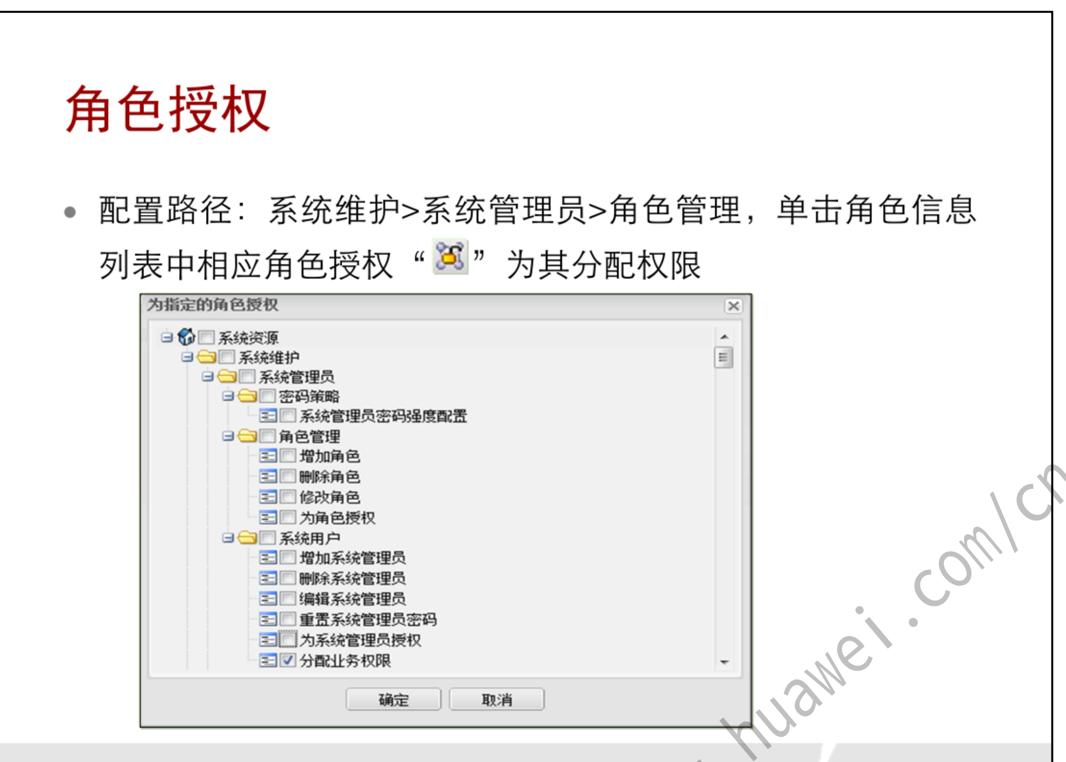
- 本节主要介绍终端安全系统维护有关操作。包括系统管理员账号及权限管理、日志管理、设备升级、定制报表，另外管理员可通过公告的形式向所有的代理用户发布通知。例如，最新的软件和补丁安装通知，公告管理本教材不做介绍，可查看产品文档。

角色增加

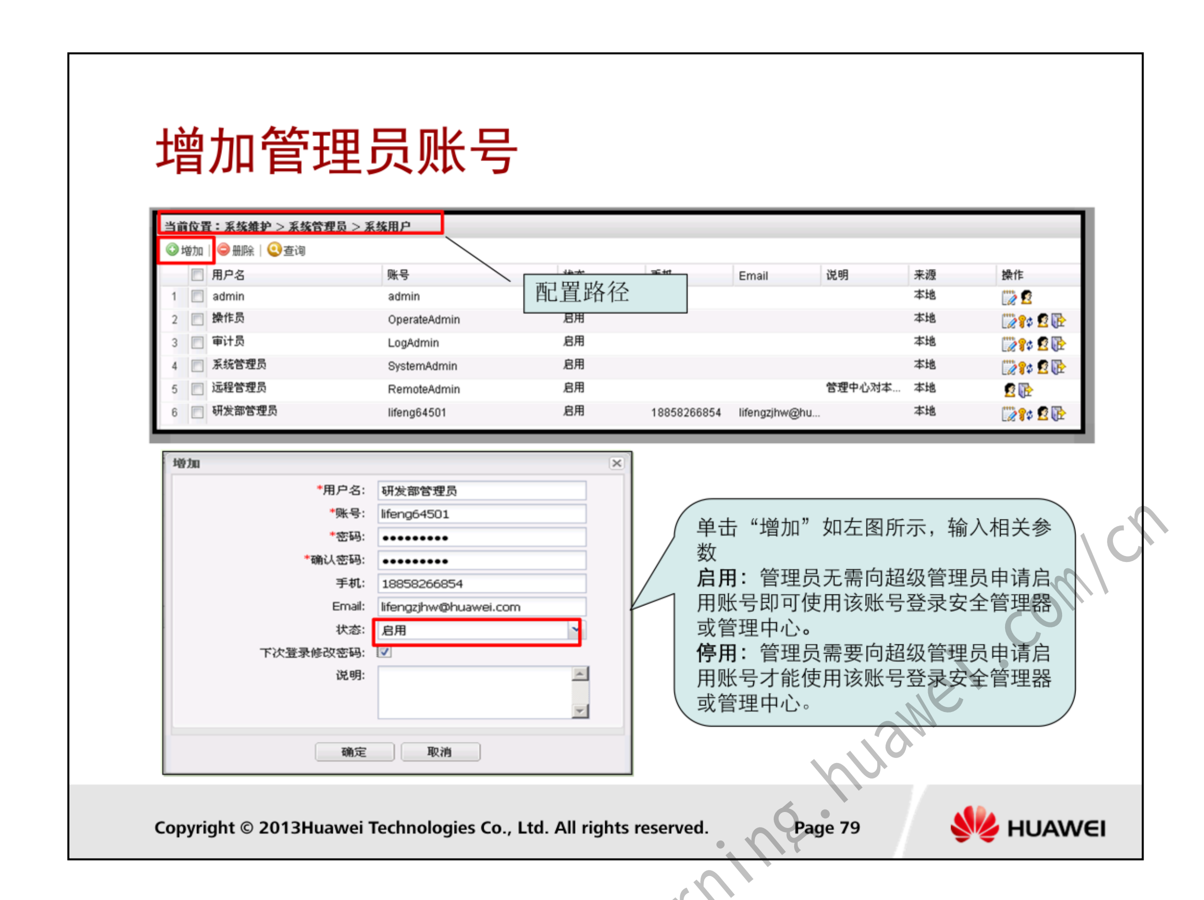
- 角色是一系列操作权限的集合。当角色分配给账号后，账号就拥有了该角色定义的所有操作权限。



- 在策略管理中心的管理和维护过程中，管理员需要根据职责分工定义多种不同的角色，并为角色授予不同的操作权限。属于同一种角色的管理员，其操作权限相同。当创建新管理员账号时，管理员只需为管理员账号授予指定角色，该账号会自动继承指定角色具有的所有操作权限。通过角色为账号授权可以避免重复劳动，减轻账号管理的工作负担。



- 对于非系统默认的管理员账号，需要分配特定的权限后，才能进行相关的业务操作。
- 授权完成以后能够操作管理器各功能模块的静态权限。对应于管理器导航栏和左侧菜单栏中各功能模块的权限



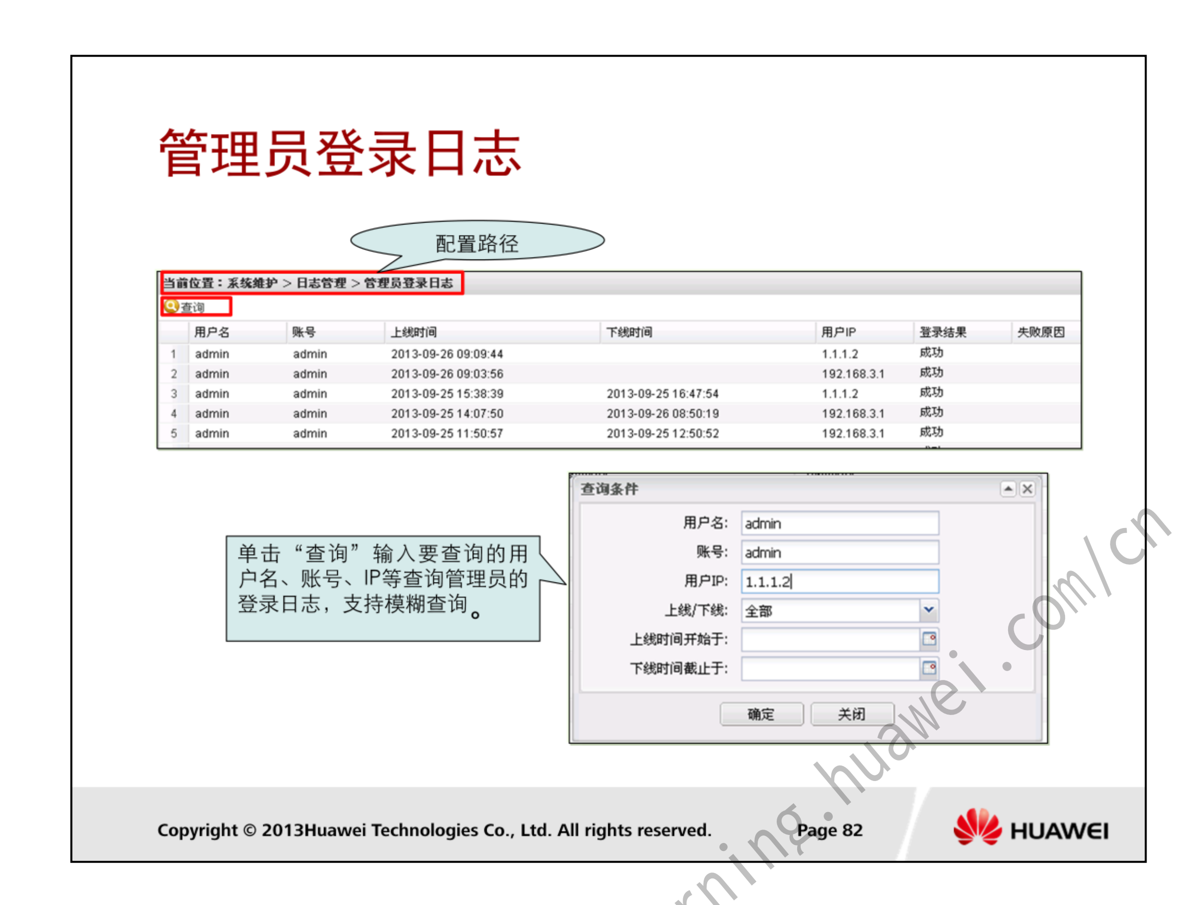
- admin是策略管理中心的超级管理员账号，用来进行权限管理和系统维护工作。为了便于按部门来维护和管理部门信息、员工信息和资产信息，通常超级管理员为每个部门创建一个管理员作为该部门的负责人，由部门的负责人统一管理和维护部门的所有信息，便于每个部门独立运作。为了便于统一管理操作权限，请根据工作所需的操作权限规划并创建不同的角色。如果安全管理器和管理中心中不包含自定义的角色，请先创建角色。
- SystemAdmin、OperateAdmin、LogAdmin、RemoteAdmin四个管理员账号只具有操作权限，还需要分配业务权限才能管理具体的部门。



- 为管理员账号授予业务权限，管理员以管理员账号登录才具有进行业务相关操作的权限。超级管理员admin具有所有权限，不能被授予业务权限。
- 为管理员账号授予角色，管理员以管理员账号登录才具有管理相关操作的权限。



- 系统日志管理包括：查询管理员账号的登录日志、增加视频监控日志、查询视频监控日志和查询SM管理器的系统日志。

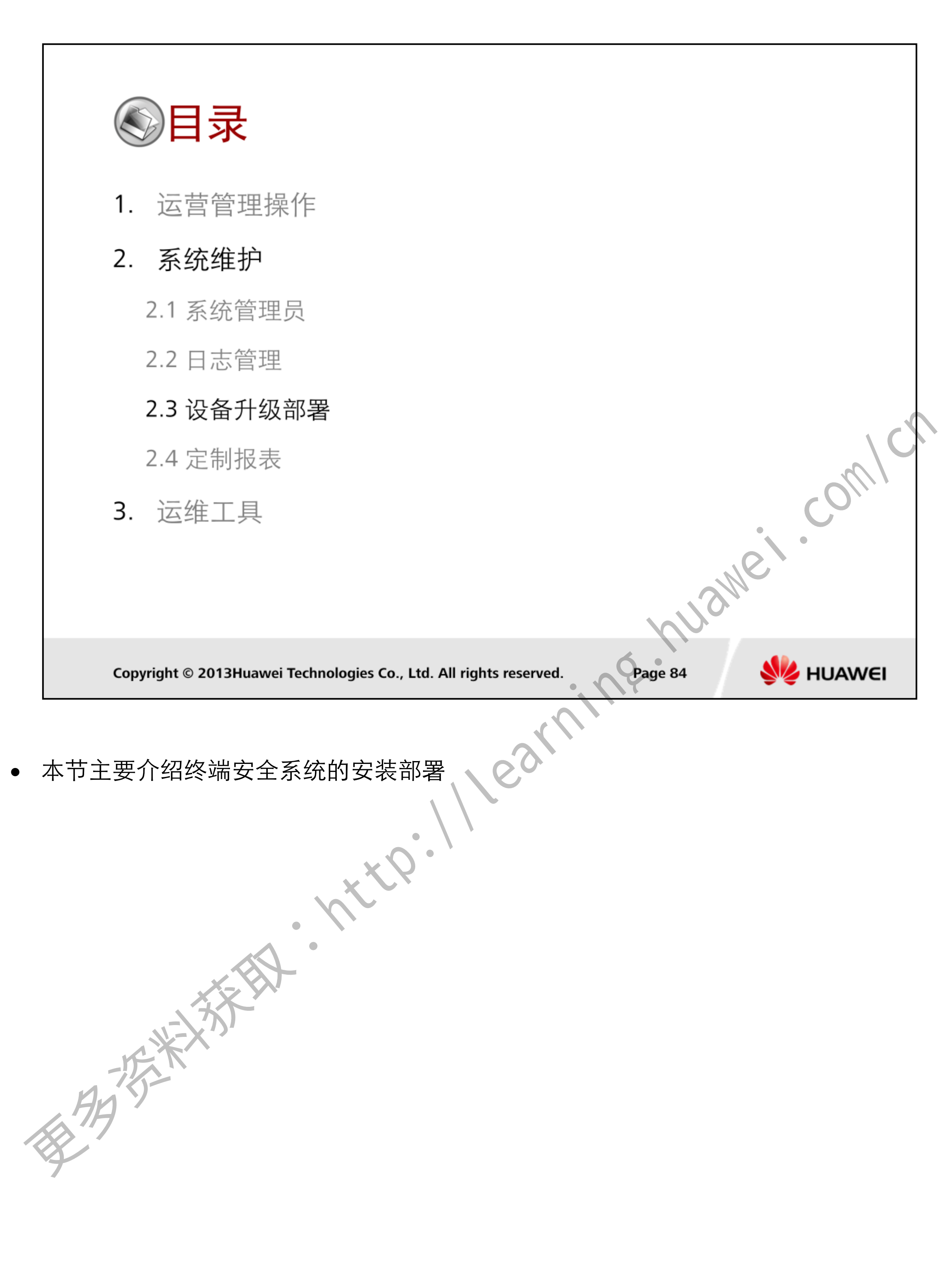


	用户名	账号	上线时间	下线时间	用户IP	登录结果	失败原因
1	admin	admin	2013-09-26 09:09:44		1.1.1.2	成功	
2	admin	admin	2013-09-26 09:03:56		192.168.3.1	成功	
3	admin	admin	2013-09-25 15:38:39	2013-09-25 16:47:54	1.1.1.2	成功	
4	admin	admin	2013-09-25 14:07:50	2013-09-26 08:50:19	192.168.3.1	成功	
5	admin	admin	2013-09-25 11:50:57	2013-09-25 12:50:52	192.168.3.1	成功	

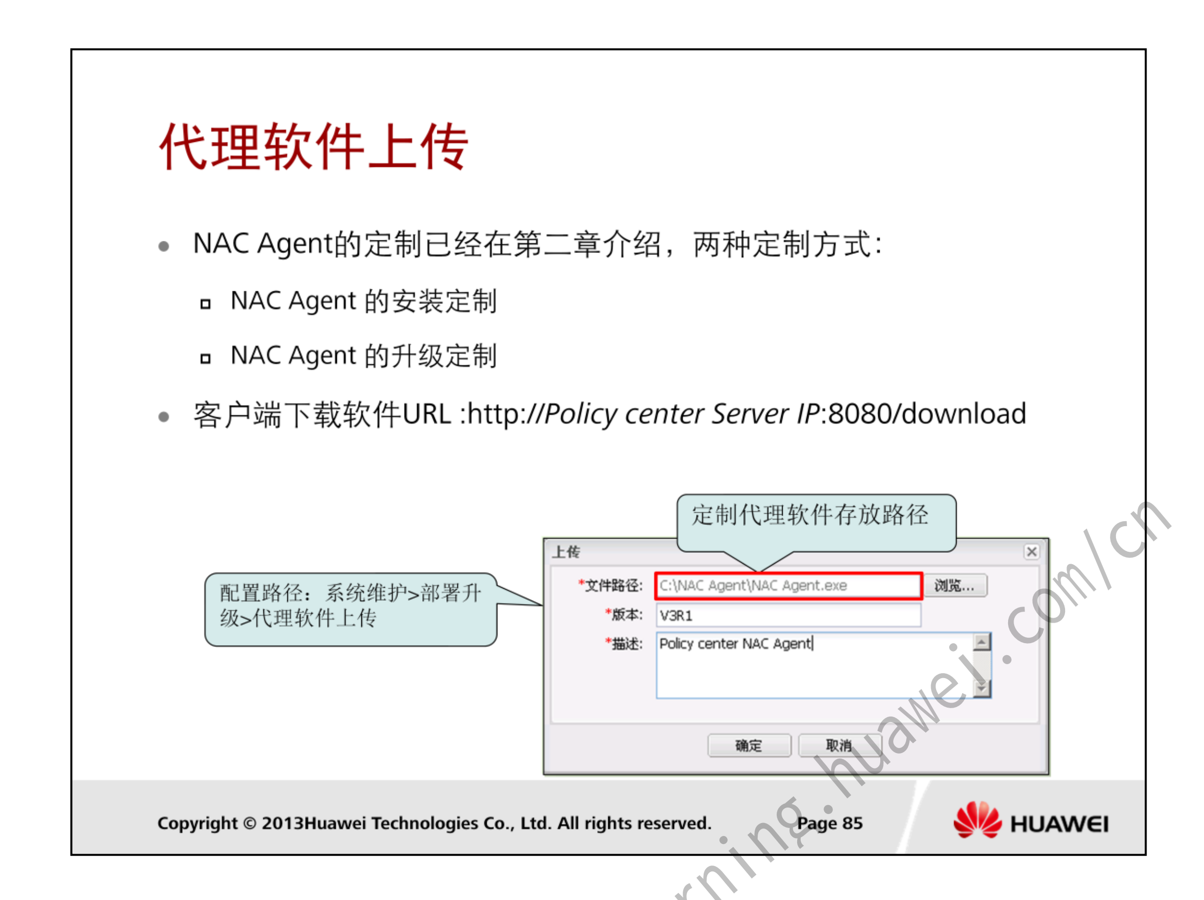
- 输入要查询的用户名、账号、IP等查询管理员的登录日志，支持模糊查询。
- 通过查询管理员账号的登录日志，可以了解各个管理员登录和登出的情况



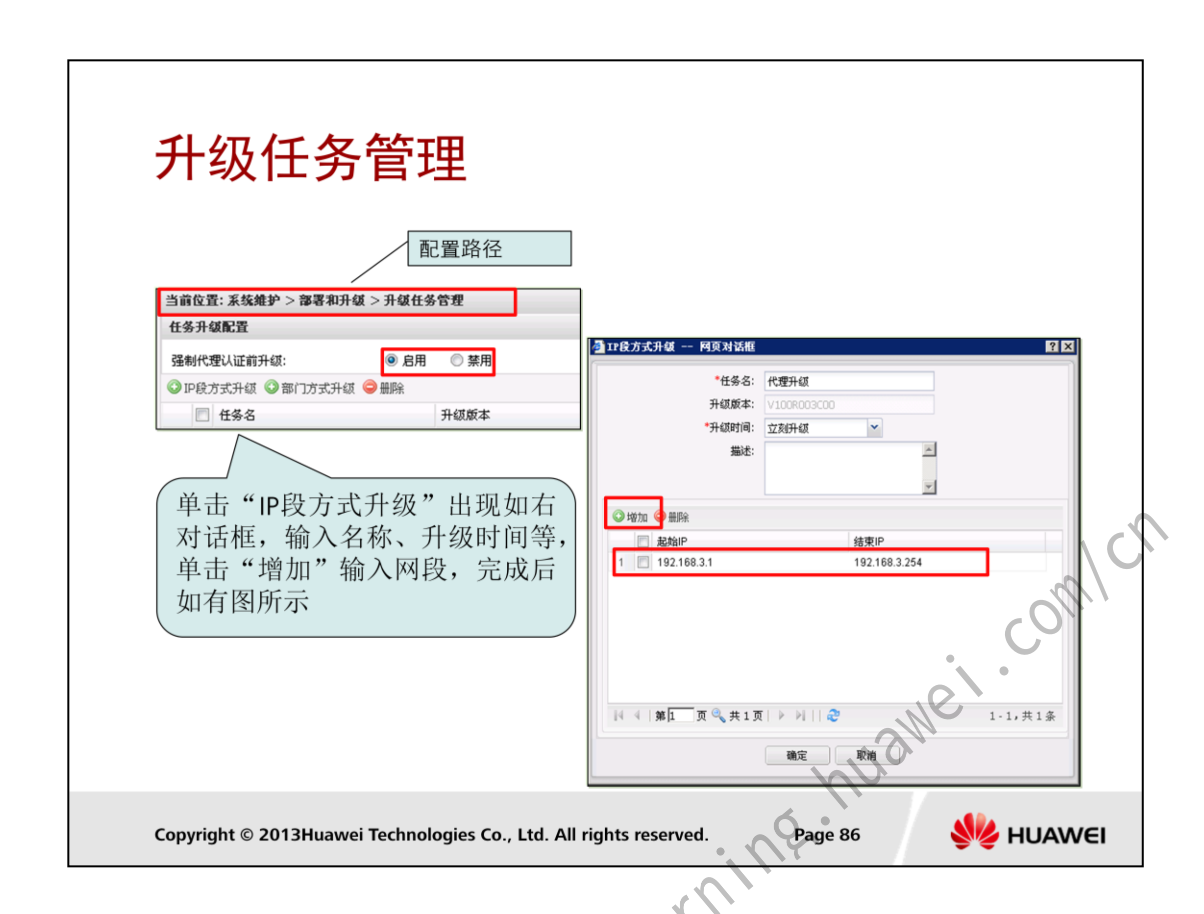
- 管理员可通过账号、操作终端IP、起始时间、结束时间、操作对象和操作名称等参数查询系统日志，及时发现异常情况。



- 本节主要介绍终端安全系统的安装部署



- 该下载界面是由SACG推送，所以在配置SACG时需进行如下配置：
  - [USG5300-rightm] right-manager authentication url http://Server IP Address:8080/download



- 升级方式有3种：
  - 强制升级：表明在不升级代理的情况下终端用户将无法继续访问网络。
  - 非强制升级：表明在不升级代理的情况下终端用户依然能够访问网络。
  - 手动升级：由终端用户手动运行新版本的代理安装程序实施版本升级。



- 本节主要介绍终端安全系统终端安全评估报表定制。

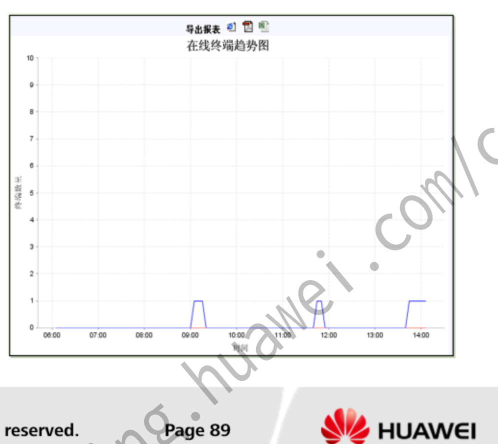


- 策略管理中心默认支持以下报表模板：
    - 安全事件评分统计图 对指定部门及其一级子部门在指定时间内所有策略进行统计得出的评分。得分越高，表明该部门在指定时间内的策略违规越少。
    - 终端状态统计图 统计当前在线无违规、在线有违规但未被隔离、在线有违规并且被隔离和未上线终端主机的数量分布饼图。
    - 终端安全趋势图 截至统计时间的最近30天内，统计指定策略的违规数量。
    - 安全事件TopN分析图 统计指定部门及其一级子部门在指定时间内某条策略的违规次数。
    - 安全策略违规状态图 统计当前在线终端主机违规数量最多的前5条策略。
    - 安全策略隔离状态图 统计当前被隔离在线终端主机数量最多的前5条策略。
    - 在线终端趋势图 统计指定时间段内在线终端主机与被隔离域终端主机的数量

即时报表管理

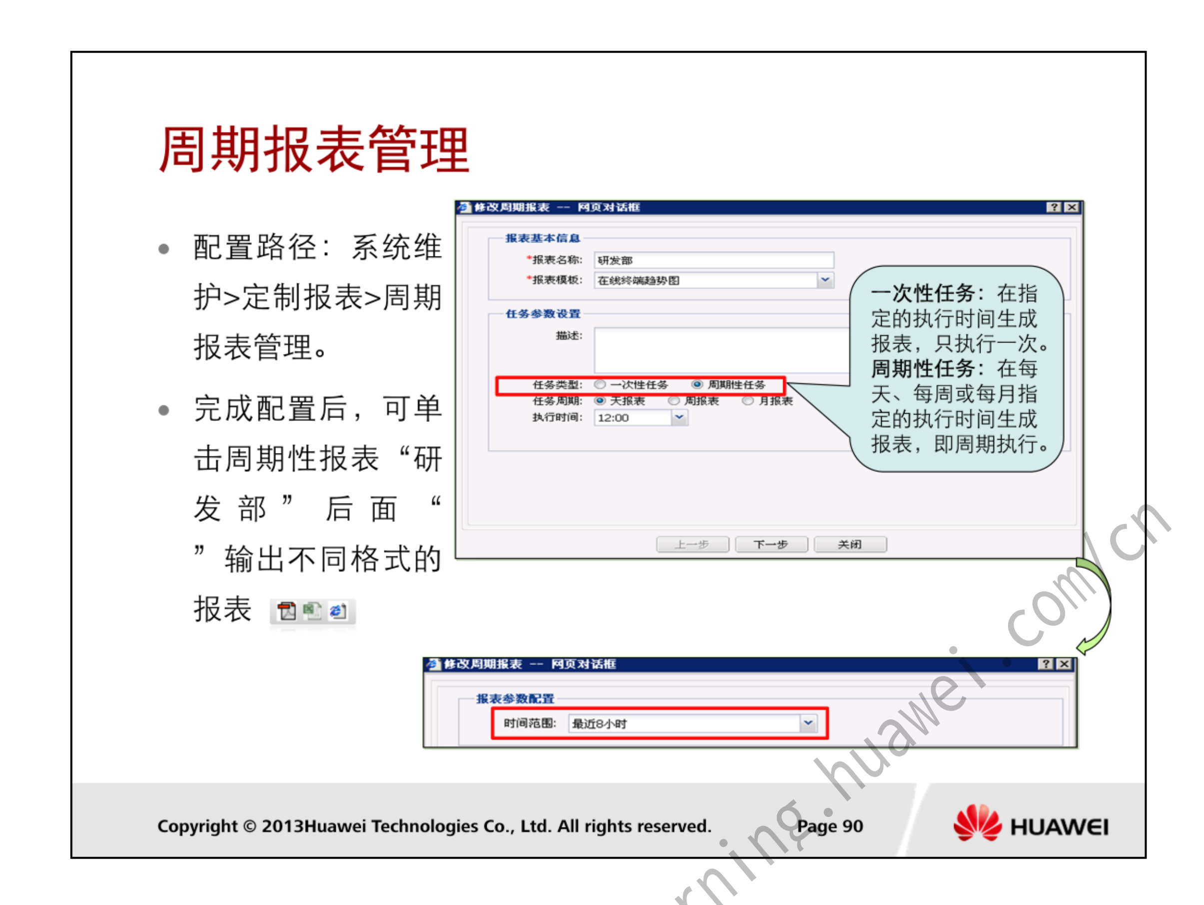
- 配置路径：系统维护>定制报表>及时报表管理，单击右侧报表栏中“增加”输入名称，模板选择“在线终端趋势图”单击“确定”单击“ ▶ ”可看到终端在线趋势。





HUAWEI

- 即时报表指立即能生成的报表。管理员可以在创建完即时报表后，立即执行或者随时执行报表，以便迅速了解当前最新的报表信息。



- 通过创建周期报表，系统会根据指定的执行时间定时生成报表。
- 选择使用哪一种报表模板生成报表。策略管理中心默认的报表模板中，周期报表只支持以下报表模板：
  - 在线终端趋势图
  - 安全事件评分统计图
  - 安全事件TopN分析图
  - 终端安全趋势图
- 选择“在线终端趋势图”时，需要设置以哪个时间段统计“在线终端趋势图”，支持选择以下时间段：
  - 最近1小时
  - 最近2小时
  - 最近4小时
  - 最近8小时
  - 最近12小时



- 本节主要介绍终端安全系统运维工Server Monitor的使用。

Server Monitor简介

- Server Monitor是查看Policy Center管理器或控制器的运行状态信息的一款工具，当管理器或制器出现异常时，Server Monitor将会产生告警，帮助管理员尽早发现故障。
- 应急处理：当发生严重故障，可以利用该工具手工开启逃生通道

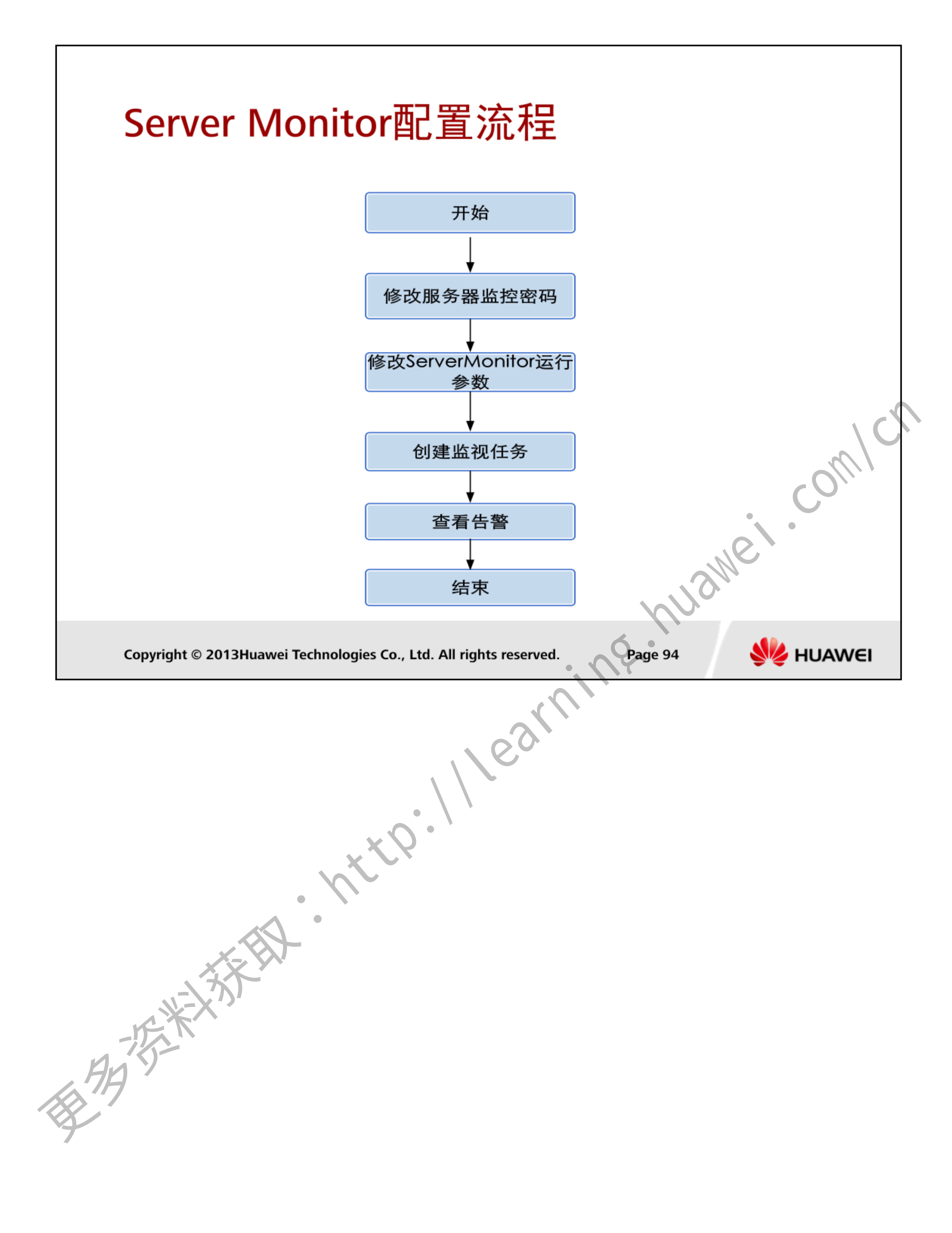


Server Monitor是查看Policy Center管理器或控制器的运行状态信息的一款工具，当管理器或制器出现异常时，Server Monitor将会产生告警，帮助管理员尽早发现故障，在收到Server Monitor产生的告警信息后，管理员需要仔细分析告警信息并判定管理器或控制器是否确实产生故障。对于已经影响Policy Center正常运行的故障，管理员需要立即采取应对措施，为恢复故障争取宝贵的时间，另外通过防火墙助手工具可以实现在交付阶段分网段进行业务割接功能，Server Monitor监控项目主要有：

- 服务器连接状态
  - 检查Server Monitor与管理器之间的连接状态，检查Server Monitor与控制器之间的连接状态。
- SC 连接状态。
  - 仅适用于管理器或管理器+控制器，检查管理器控制器之间的连接状态，如果管理器与控制器连接失败，Server Monitor将会告诉管理员控制器的IP地址。
- SACG 连接状态
  - 检查控制器与安全接入控制网关之间的连接状态，如果控制器与安全接入控制网关连接失败，Server Monitor将会告诉管理员安全接入控制网关的IP地址。
- 包括TCP连接数、License信息，以及终端数量等都是监控的项目。


Server Monitor安装
运行ServMonSetup.exe，选择安装语言：中文（简体）出现如右图安装向导，单击“下一步”完成安装。
安装程序语言
请选择安装程序语言
中文(简体)
OK
Cancel
Server Monitor
欢迎使用Server Monitor V2.1安装向导
这个向导将指引你完成“Server Monitor”的安装进程。
在开始安装之前，建议先关闭其它所有应用程序。这将允许“安装程序”更新指定的系统文件。
单击[下一步(N)]继续。
Install
< 上一步(P)
下一步(N) >
取消(C)
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 93
HUAWEI

- 使用安装向导完成安装。



Server Monitor配置流程
开始
修改服务器监控密码
修改ServerMonitor运行参数
创建监视任务
查看告警
结束
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 94
HUAWEI



- 密码管理员自定义，但是必须要与Server Monitor的密码配置一致，两者才可以联动成功。



- 设置Server Monitor的系统参数，以便管理员修改Server Monitor的启动方式、告警检查周期、对话框告警开关的状态、对话框告警间隔时间、邮件告警和短信告警开关的状态。



- 注意密码的配置需与Policy Center的配置相同。



- 在众多告警信息中，过滤告警项目监视任务中剔除不关注的告警项目，以便管理员只收到关注的告警项目的告警信息，避免告警过多而忽略重要的告警。
- Server Monitor可以配置邮件、短信通知管理员及时处理告警。

目录



- 本节主要介绍扫描器的使用。

扫描器简介

- 设备扫描是指网络管理员通过软件或硬件在网络中进行探测并发现设备类型、名称、地址和数量，方便网络管理员了解整个网络中的设备类型和数量，扫描器使用场景：
  - 在部署Agent代理之前，创建一次性的扫描任务，收集设备分类和数量。
  - 在部署Agent代理时，创建周期性的扫描任务，用于评估Agent代理的部署进度
  - 在部署Agent代理后，创建周期性的扫描任务，用于收集新设备接入网络和卸载Agent代理的告警。



- 扫描器的作用：
  - 管理员在部署NAC Agent代理前收集整个网络的设备类型和数量，发现网络中没有部署代理的终端主机，并协助部署代理。 在部署代理前，汇总终端主机的数量，以便管理员初步评估代理的部署进度安排。在部署阶段，便于管理员评估部署进度和效果， 以便提醒和监督没有安装NAC Agent代理的终端用户安装NAC Agent代理。
  - 利用扫描结果快速配置例外设备。 设备扫描帮助管理员发现并放行不适合进行接入控制的设备。例如，管理员无法在IP Phone、打印机、门禁系统等特殊设备（称之为例外设备）上安装代理，而这些设备在正常工作时需要访问网络。在启用终端主机接入控制后，这些例外设备因未通过身份认证导致无法访问网络，进而无法为终端用户提供服务。此时，管理员通过对设备扫描结果中的未知设备进行分析和排查，并把例外设备加入认证前域，确保例外设备能够正常访问网络。
  - 对新接入网络的设备或卸载代理的终端主机进行告警。 对于新发现的设备接入网络，或者发现终端用户卸载代理，扫描器产生告警，提醒管理员关注新接入网络的设备或卸载代理的终端主机，评估此事件对网络安全的影响。


扫描器安装（1）
运行DeviceScannerSetup.exe，选择安装语言，单击“下一步”。
安装程序语言
请选择安装程序语言
中文(简体)
OK
Cancel
Device Scanner
欢迎使用Device Scanner V2.0安装向导
这个向导将指引你完成“Device Scanner”的安装进程。
在开始安装之前，建议先关闭其他所有应用程序。这将允许“安装程序”更新指定的系统文件，而不需要重新启动你的计算机。
单击［下一步(N)］继续。
Install
< 上一步(P)
下一步(N) >
取消(C)
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 101
HUAWEI

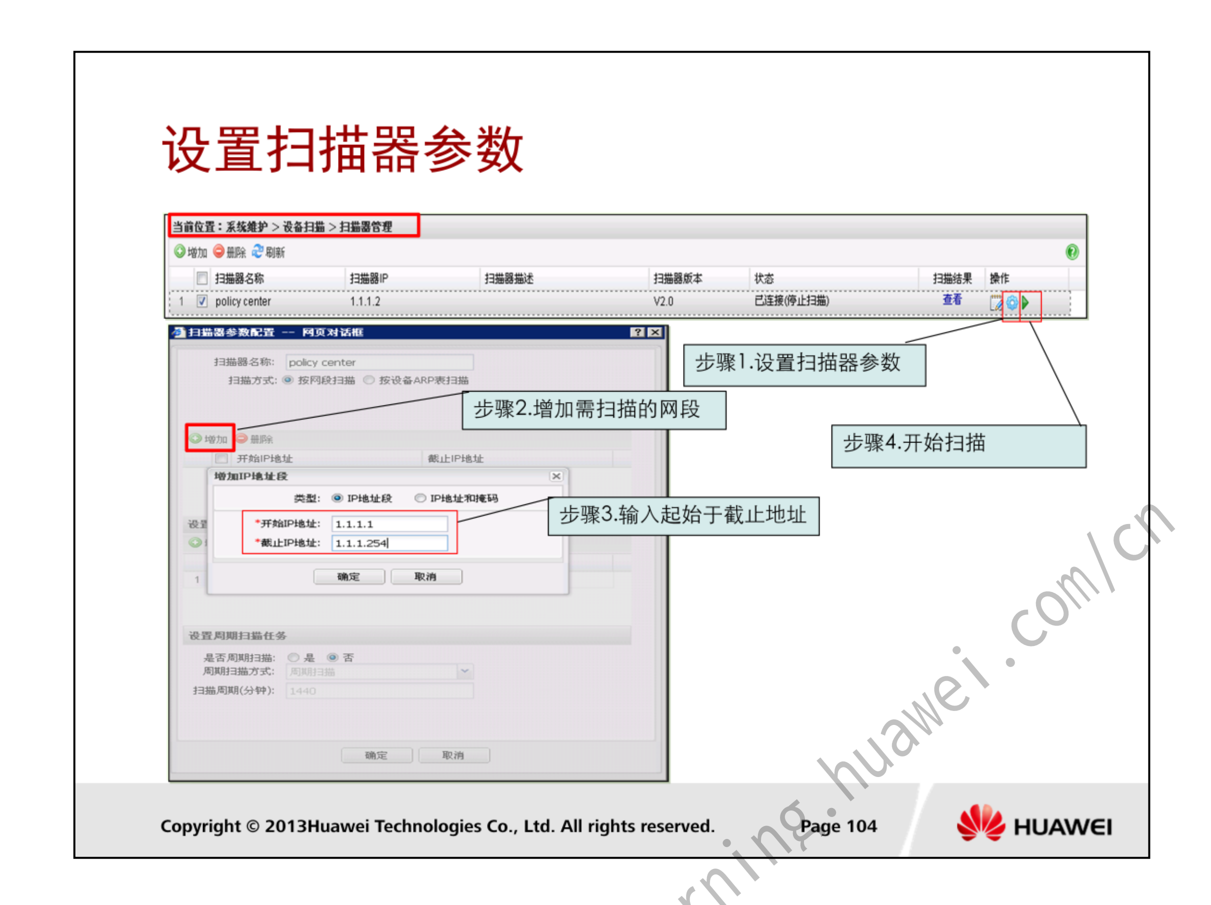
- 按照安装向导完成安装。



- 扫描器与策略中心联动需输入管理器IP地址，需保证扫描器所在设备与Policy Center管理器路由可达。



- 输入扫描器所在设备可用IP地址，注意：本例中扫描器与Policy Center管理器，安装在同一台设备上故IP地址配置相同。



- 按网段扫描设备，适用于在指定的网段范围内进行设备发现的场合。
- 按网段扫描设备，首先需要确定目标网段的IP地址范围。如果管理器管辖范围内部署了多台扫描器，在为不同的扫描器配置扫描参数时，为了提升设备扫描效率，各台扫描器扫描的IP地址段不要重叠。
- 为了扫描器能够获取交换机或路由器的详细信息，管理员还需要获取交换机或路由器的SNMP只读团体字。交换机或路由器在向网管（这里是指扫描器）上报自身的信息之前，会检查网管提供只读团体字与设备自身的只读团体字是否匹配，以验证扫描器是否有权限读取本设备的信息。

查看扫描结果

- 查看路径，系统维护>设备扫描>设备管理，可以看到安装代理的主机信息与没有安装代理的主机信息。
- 同还可以对扫描发现的设备加入相应的组，便于管理。



	设备名	IP地址	MAC地址	设备类型	安装代理	标记免安装代理	最近扫描时间
1	HUAWEI-23EBEB99	1.1.1.2	00-1E-90-B3-05-80	PC设备	未安装		2013-10-08 16:14:07
2	lwx64015	1.1.1.1	E8-9A-8F-B0-C6-B0	PC设备	已安装		2013-10-08 16:13:46

- 建议按用途对已发现的设备进行分类，方便管理员对设备进行分类管理和分类查询。



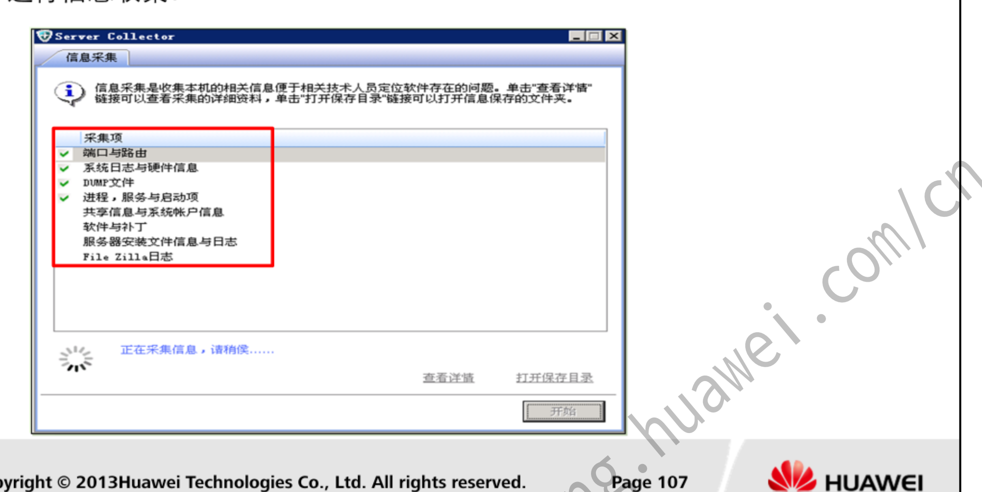
目录



- 本节主要介绍信息采集工具使用。

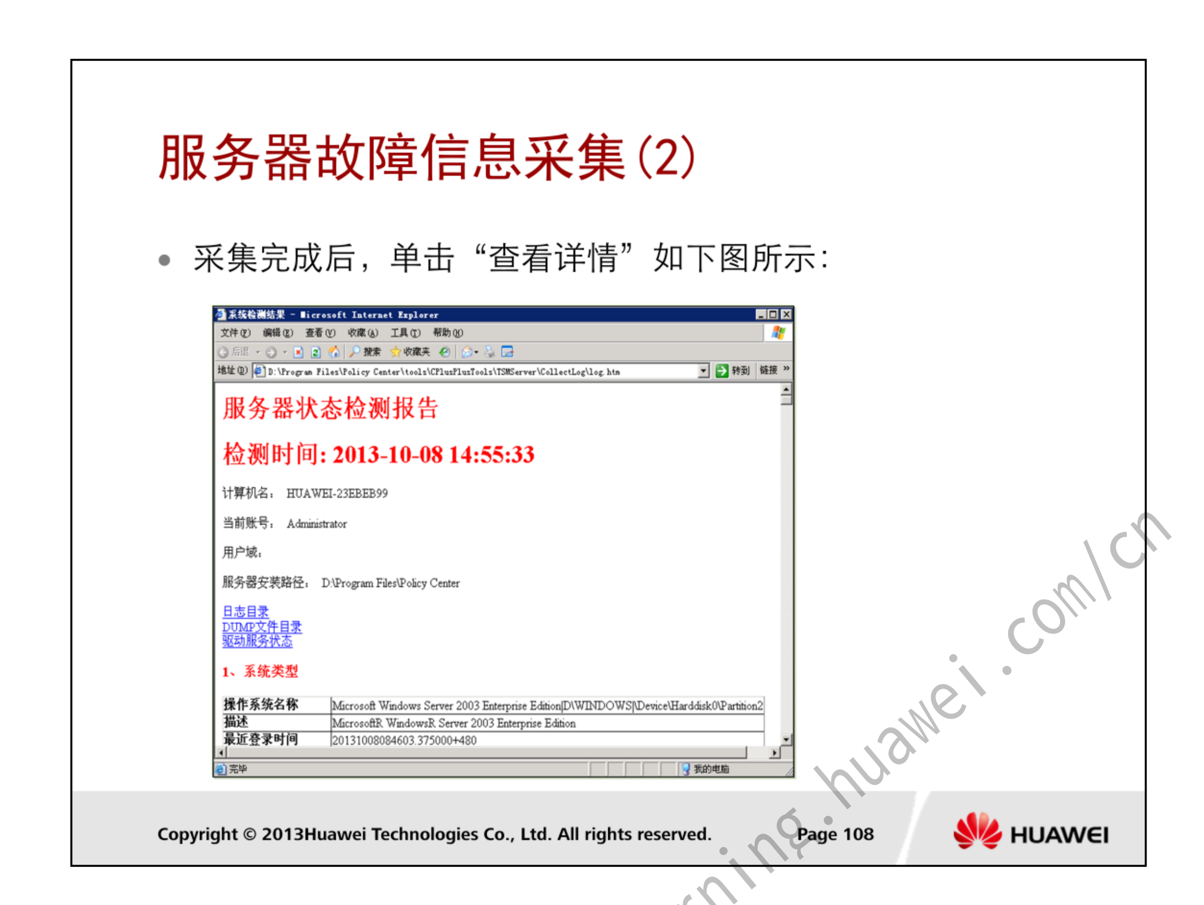
服务器故障信息采集（1）

- 使用 “administrator”账号登录Microsoft Windows Server 2003操作系统，选择 开始 > 程序 > Huawei > Policy Center > Server Collector，单击 “开始”进行信息收集。

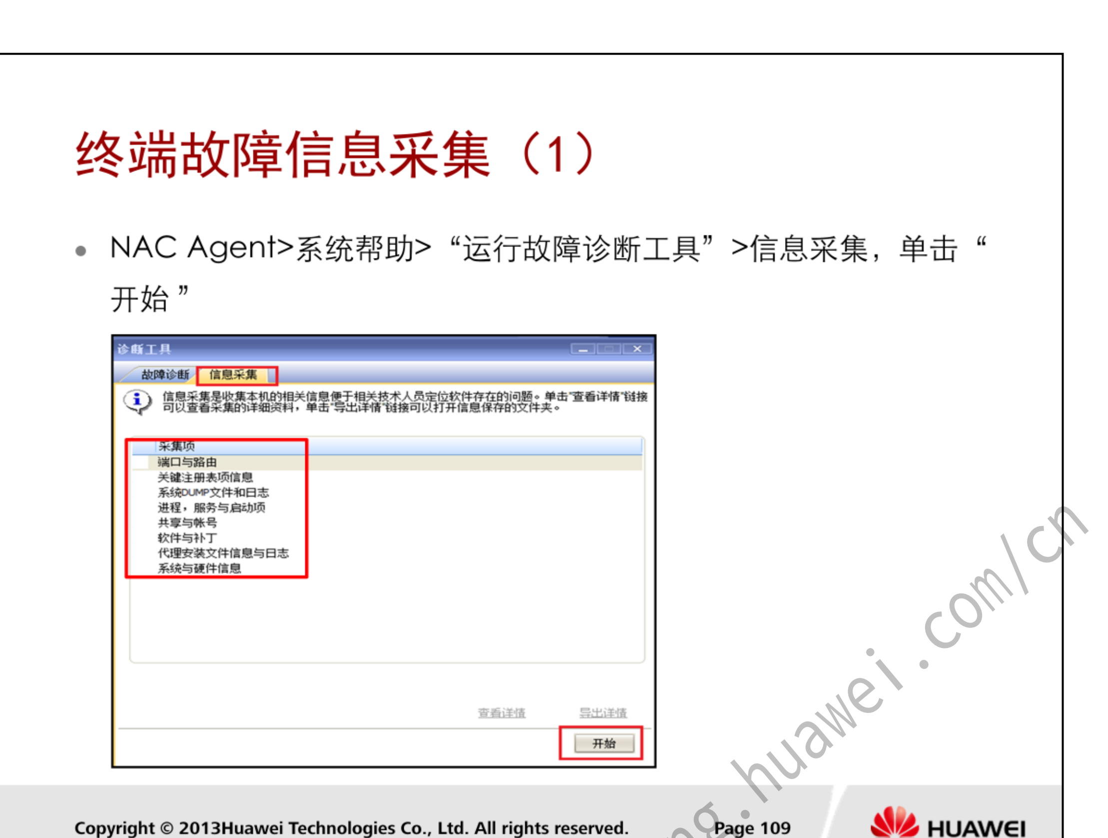




- 当服务器出现故障可以使用该工具，方便问题定位。



- 可以查看到服务器设备信息，操作系统信息、软硬件信息等。



- 当代理出现故障后，终端用户使用管理员账号运行故障诊断工具，在采集故障信息时，选择将故障采集结果存放在桌面。故障信息采集完成后，终端用户单击“导出详情”，查看采集结果，弹出的桌面窗口中没有log.zip文件。



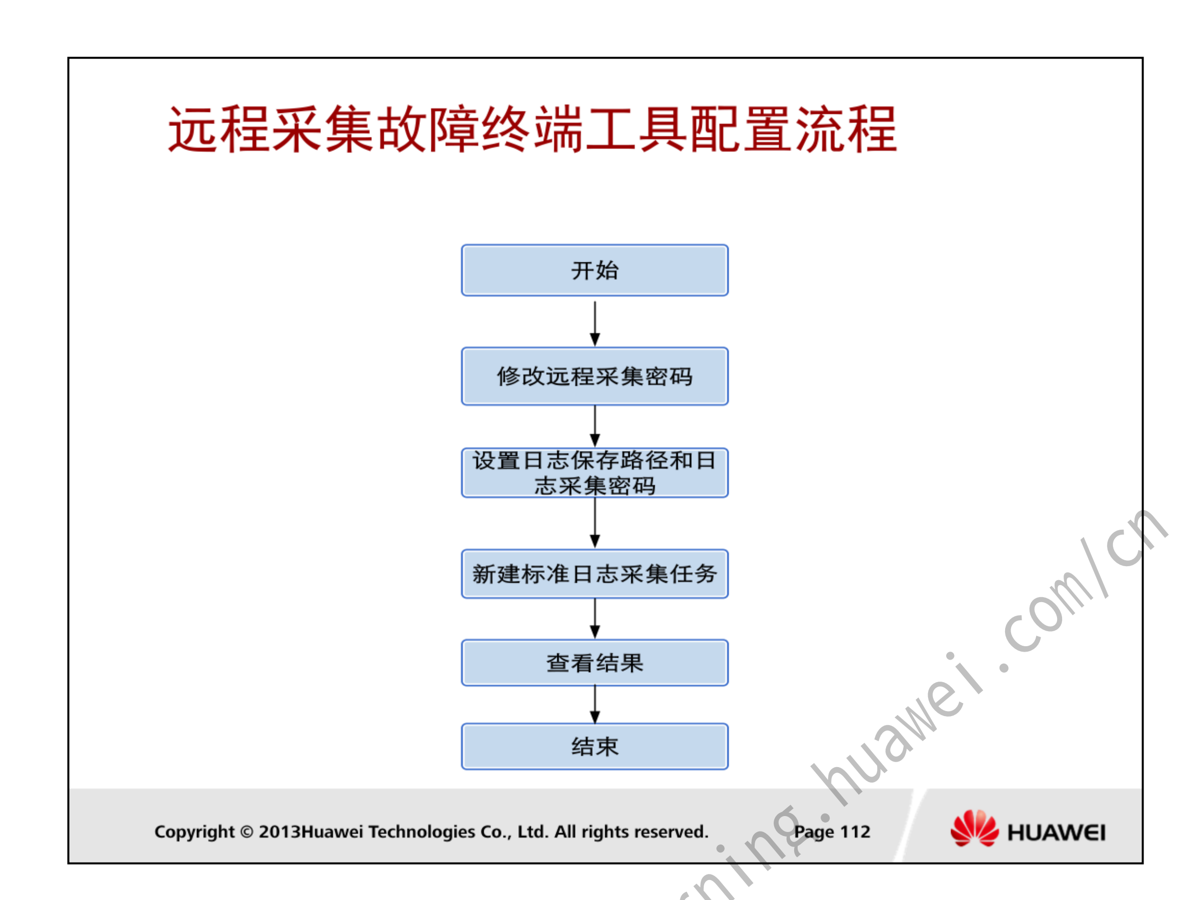
- 通过代理故障诊断工具收集代理与故障相关的信息，然后提交给管理员或华为技术工程师帮助定位故障。

远程采集故障信息工具

- 运行Remote Log Collector.exe（为了防止滥用，该程序安装在SM和SC服务器上）



- 远程日志采集工具是策略管理中心管理员用于远程采集终端主机日志的工具，适用于以下场景：NAC客户端无法正常工作，管理员不方便到故障现场，并且不方便指导终端用户使用NAC客户端诊断工具，从而通过远程方式采集与诊断NAC客户端故障相关的日志。



远程采集故障终端工具配置流程
开始
修改远程采集密码
设置日志保存路径和日志采集密码
新建标准日志采集任务
查看结果
结束
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 112
HUAWEI



- 通信口令默认为Admin@123，该口令需与采集工具配置相同，两者才能联动。



- 注意：日志采集密码为Admin@123需与Policy Center的口令相同。



- 建立单点采集任务输入终端IP地址，即知采集一台终端的日志信息，当然可以采用“IP段采集”，在采集模式选择标准采集。



检查结果

- 当日志采集任务执行成功后，双击日志采集任务，查看所采集的终端主机日志。界面显示日志文件的存放目录。单击Log.rar>Log.htm

系统检测结果 - Microsoft Internet Explorer

状态检测:系统检测报告 -- 采集时间: 2013/10/8 15:37:55

计算机名： LWX64015

当前账号： SYSTEM

用户域： china.huawei.com

代理安装路径： C:\Program Files\Huawei\TSM Agent

代理安装日期： 2013-10-08

代理版本： V100R003C00

当前账号类型： 普通账号

普通账号：

是否启用802.1X： 否



HUAWEI

- 可以看到用户终端主机软硬件信息，登陆方式等。



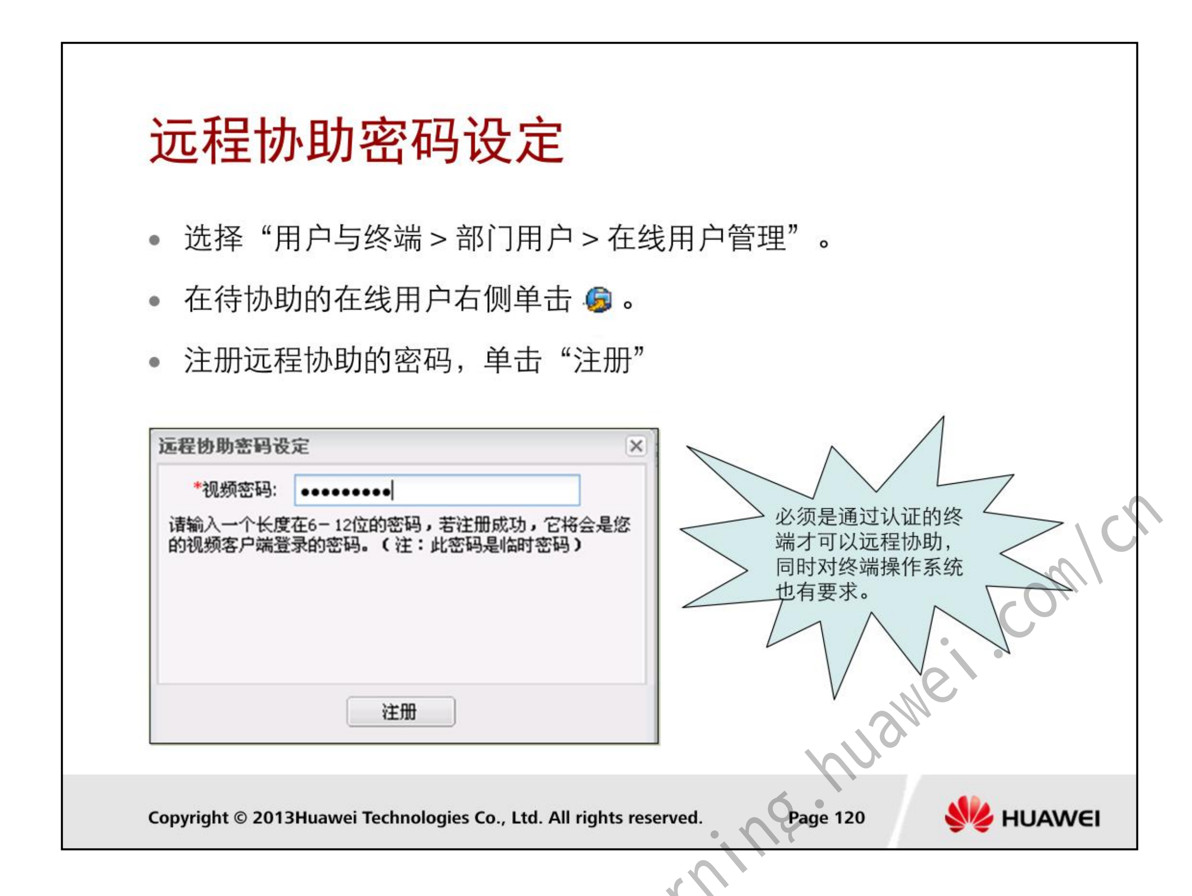
- 本节主要介绍终端安全系统远程协助工具，通过该功能的使用，管理员可以远程登陆到终端主机进行操作，方便运营维护。



- 设置远程协助参数，以便管理员能够远程控制或查看终端主机。同时，设置是否允许终端用户在代理修改远程协助参数。


分配远程协助模板
完成模板配置后，单击远程协助模板后面 分配模板给研发部，单击“确定”。
分配部门,账号,终端IP地址范围
说明：
强烈建议不要同时给部门和网络区域配置终端参数，否则将不容易识别某个终端实际使用的模板，导致管理混乱。
生效优先级：账号>网络区域>部门。
分配给部门
分配给账号
分配给终端IP地址范围
该模板已分配给下列部门（如果选择父部门，则子部门继承父部门设置。）
部门树
部门列表
移除
部门
描述
ROOT\Guest\研发部
确定
取消
Page 119
HUAWEI

- 分配改模板到研发部。



- 对于终端主机的操作系统类型的要求 管理员只能对采用如下操作系统类型的终端主机进行远程协助：
    - Microsoft Windows 2000
    - Microsoft Windows Server 2003
    - Microsoft Windows XP 32位和Microsoft Windows XP 64位
    - Microsoft Windows 7 32位和Microsoft Windows 7 64位
    - Microsoft Windows 8
    - Microsoft Windows Vista
- 在使用远程协助功能时，管理员需要输入该密码作为连接终端主机的凭证。该密码的有效期为：
    - 从注册密码开始，有效期持续30分钟，逾期密码将会失效。
    - 如果管理员使用""连接终端主机成功，则该密码立即失效。



- 单击Kvmviewer.exe下载远程协助客户端。如果已经下载，则不需此步操作，单击“提交日志”



- 权限设置，View Only只有查看权限，设置更多参数可单击“Options”。



总结

1. 终端安全系统的运营管理操作；
2. 终端安全系统配置；
3. 终端安全系统维护配置；
4. 常用运维管理工具的使用





思考题

- 代理软件上传与软件分发的区别?
- 进行策略模板配置时，继承父模板的结果是什么?
- Web Agent客户端是否可以进行远程协助?





练习题

- 判断题
  1. 对于终端安全状态进行评估，可以配置即时报表和周期性报表。
- 单选题
  1. 访客管理中访客注册后，审批方式有哪几种?

     A.免审批

     B.管理员审批

     C.接待人审批

     D.主管审批



- 习题与答案：
  - 判断题答案：错误
  - 多选题答案：ABC

Thank you

www.huawei.com

HC120320005 终端安全系统故障处理

www.huawei.com

HUAWEI



目标

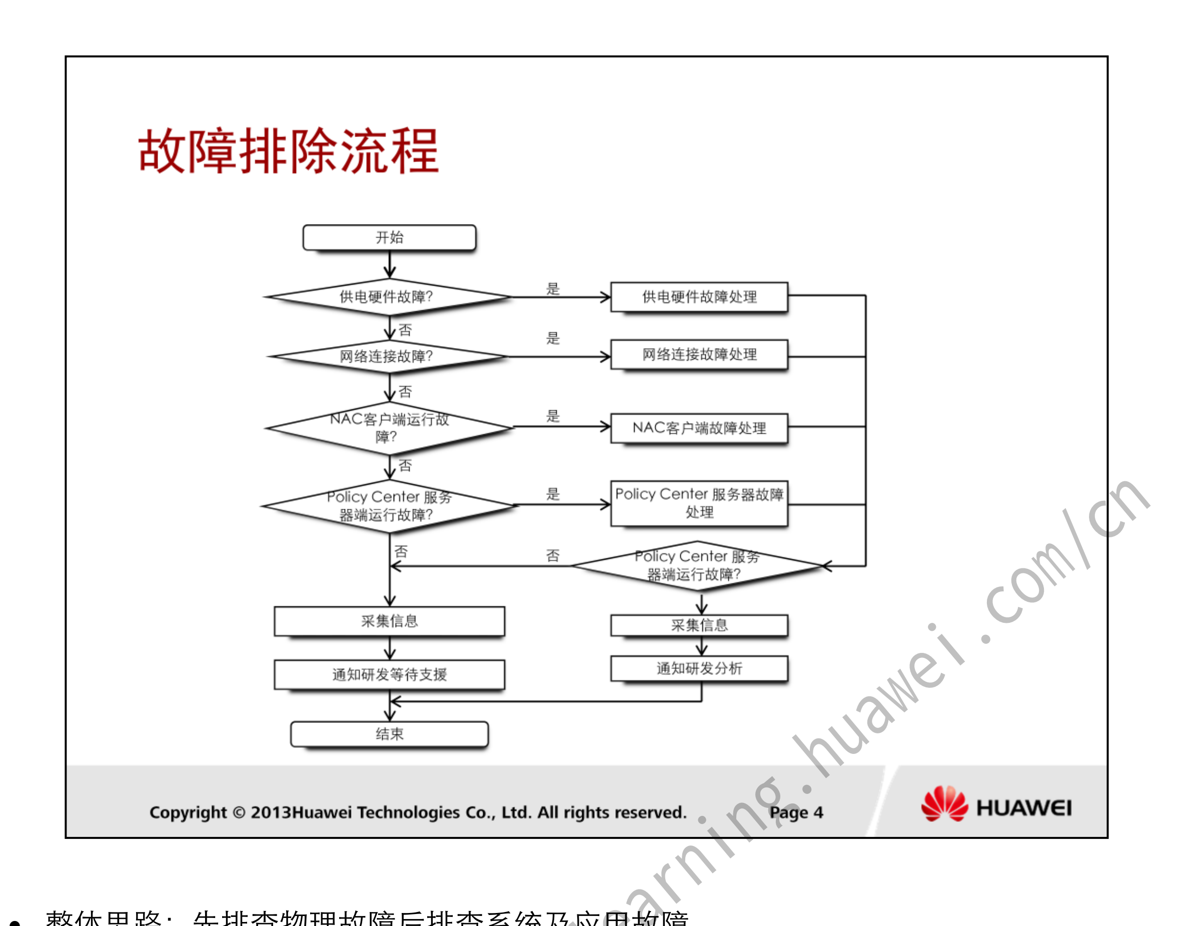
- 学习完本章节，你应该能够：
  - 了解常见的故障排除思路
  - 常握故障排除工作及使用方法
  - 掌握系统维阶段故障定位





目录





- 整体思路：先排查物理故障后排查系统及应用故障。



目录



安装过程中同步时间服务器失败

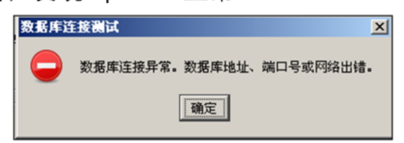
- 问题描述
  - 在安装安全管理器或安全控制器过程中，单击“设置系统参数”，在“Internet 时间”页签配置时间服务器的连接参数，单击“立即更新”后，同步时间服务器失败。
- 原因分析
  - 由于时间服务器的客户端与服务端的连接超时，或者在时间服务器同步过程中w32time服务正在启动，导致同步时间服务器失败。
- 解决办法
  - 该问题不影响策略管理中心服务器的安装。请在策略管理中心服务器安装完成后，手工进行时间服务器的同步操作。手工同步时间服务器的操作



- 手工同步时间服务器的操作如下：
  - 选择“开始>设置>控制面板”，双击“日期和时间”；
  - 单击“Internet时间”；
  - 选中“自动与Internet时间服务器同步”，并在“服务器”中输入时间服务器的域名或IP地址；
  - 单击“立即更新”；
  - 单击“确定”。
- 如果在手工同步时间服务器时仍然出现该问题，请尝试重复进行手工同步，直至同步时间服务器成功。

Policy Center服务器安装过程无法连接数据库

- 问题描述
  - 在Policy Center在安装过程中提示“连接数据库失败”，导致无法安装。登陆数据库服务器，发现SqlServer正常。



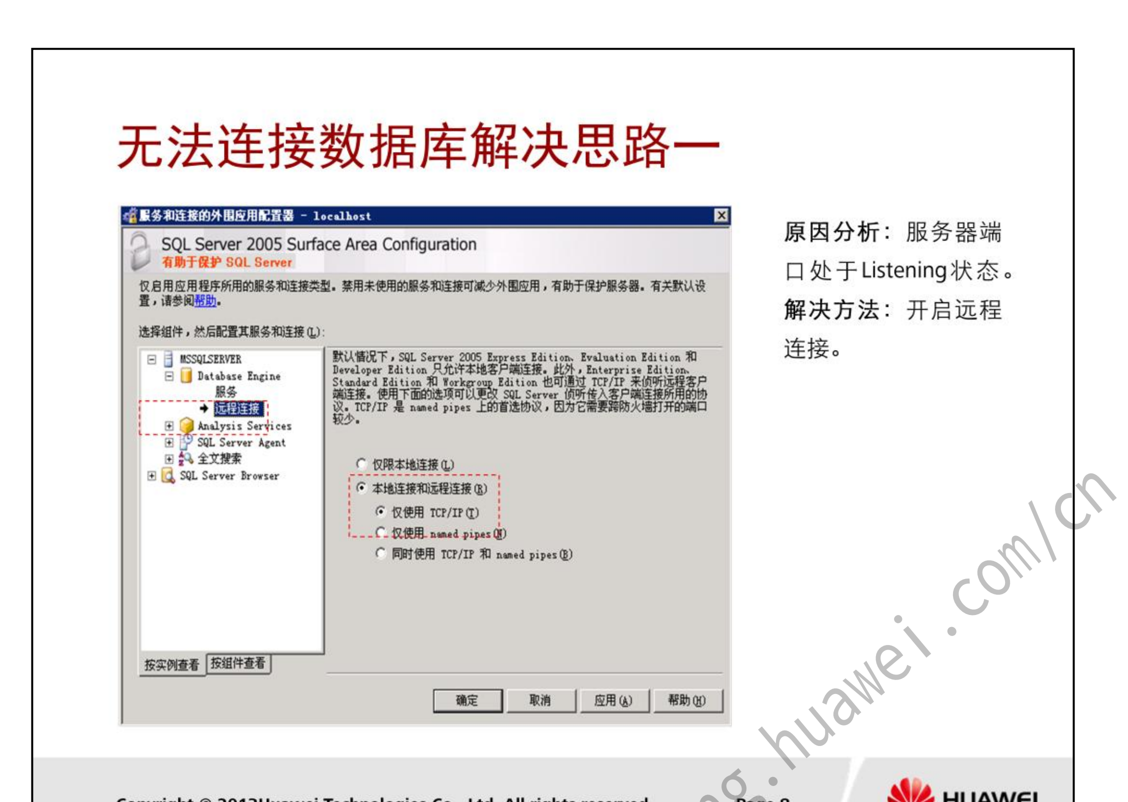
- 原因分析
  - 没有开启远程连接；
  - MSSQLSERVER协议未启用或端口设置有误。
- 解决办法
  - 开启远程连接；
  - 启用MSSQLSERVER协议或纠正端口设置错误。



HUAWEI



- 开启SQL2005远程连接功能
  - 开始菜单->程序-> Microsoft SQL Server 2005->配置工具->SQL Server Configuracion Manager
  - SQL Server2005 网络配置-> MSSQLSEREVER的协议->TCP/IP,双击打开
  - 在“协议”选项卡把‘已启用’由默认的‘否’改为‘是’
  - 在“IP地址”选项卡把最下面‘IP All’选项卡里的TCP动态端口改为空，TCP端口改为‘1433’或者您需要的端口号码。
- 启用MSSQLSERVER协议或纠正端口设置错误。
  - 在服务器上打开SQL Server Configuration Manager。单击“开始”，依次选择“程序"、"Microsoft SQL Server2005"、"配置工具"，然后单击"SQL Server配置管理器"；
  - 接着依次选择“SQL Server 2005网络配置”、"MSSQL SERVER的协议"、在右边的协议名称中查看，除VIA协议外，其他协议是否全部启用；
  - admin查看TCP/IP协议的端口是否正确。右键TCP/IP协议项，选择属性，IP地址项，查看端口是否跟测试连接的端口一致。



- 根因分析：
  - 通过查看SQL服务器端口发现服务正处于Listening状态，在本服务器通过telnet SQL-ip1433发现端口不可达，但通过telnet127.0.0.1433端口则可达，那么可确定是远程连接未启用引起。
- 解决方法：
  - 依次选择“开始” -> “程序” -> “Microsoft SQL Server 2005” ->"配置工具"，然后单击"SQL Server外围应用配置器"；
  - 在"SQL Server外围应用配置器"页上，单击"服务和连接的外围应用配置器"；
  - 在“服务和连接的外围应用配置器”页上，展开“DatabaseEngine”(数据库引擎)，单击“远程连接，选择”本地连接和远程连接“复选框，选择适用于您的环境的相应协议(我这里使用TCP/IP)，然后单击”应用“。(注意:请在接收到以下消息时单击“确定”。至左栏“服务”进行重新启动数据库引擎服务，使连接设置所做的更改生效。)；
  - 也可通过在本地数据库服务器设置，选择数据库节点->右键属性->安全性->服务器身份认证，选择SQL Server和windows身份验证模式。



- 根因分析：
  - 通过查看SQL服务器未发现1433端口处于Listening状态，通过“任务管理器”查找sqlservr.exe进程所对应PID，然后在本服务器通过netstat – ano将能找到PID及对应的服务端口。
- 解决方法：
  - 在服务器上打开SQL Server Configuration Manager。单击“开始”，依次选择“程序"、"Microsoft SQL Server2005"、"配置工具"，然后单击"SQL Server配置管理器"；
  - 接着依次选择“SQL Server 2005网络配置”、"MSSQL SERVER的协议"、在右边的协议名称中查看，除VIA协议外，其他协议是否全部启用；
  - admin查看TCP/IP协议的端口是否正确。右键TCP/IP协议项，选择属性，IP地址项，查看端口是否跟测试连接的端口一致。

远程加固服务器导制安全控制器出现故障

- 问题描述
  - 使用服务器加固工具SetWin2003加固MicrosoftWindowsServer2003操作系统后，发现安全控制器失效，无法处理终端用户的身份认证请求。
- 原因分析
  - 通过远程桌面连接至MicrosoftWindowsServer2003操作系统，使用加固工具SetWin2003加固MicrosoftWindowsServer2003操作系统，远程连接会话权限与硬件服务器本机会话不一致导致安全控制器网络连接出现故障。



- 解决办法
  - 卸载SetWin2003恢复原先设置，重启操作系统后通过“administratror”帐号以本地方式登录操作系统安装与操作SetWin2003进行系统加固。



- 解决步骤：
  - 以“administrator”账号登录Microsoft Windows Server2003；
  - 在SetWin2003的主窗口单击“退出”，停止SetWind2003；
  - 选择“开始>程序>SetWin2003>Uninstall”进行卸载SetWin2003恢复原设置；
  - 选择“系统>恢复”，开始恢复以前的设置。出现提示“手工进行恢复”操作，表示该系统模块必须手工修改才会恢复执行安全加固之前的参数值；
  - 重新启动操作系统之后，重复执行步骤一和二继续完成卸载SetWin2003；
  - 重新启动操作系统之后，以“administrator”账号以本地方式而非远程桌面方式登录MicrosoftindowsServer2003，重新安装SetWin2003并进行操作系统加固。

安全管理器或安全控制器卸载界面无法显示

- 问题描述
  - 管理员在相应目录下执行卸载安全管理器或安全控制器，无卸载界面，即在“开始”菜单选择“开始 > 程序 > Huawei > Policy Center > Uninstall or Delete Components”。但无法显示卸载对话框。
- 原因分析
  - 未修改数据执行保护导致无法访问安全管理器或安全控制器的登录页面，也无法卸载安全管理器或安全控制器。
- 解决办法
  - 修改数据执行保护，再重新启动MicrosoftWindowsServer2003操作系统，最后再执行卸载操作。



- 管理员执行如下操作无法卸载安全管理器或安全控制器
  - 使用“administrator”账号登录MicrosoftWindowsServer2003操作系统；
  - 在“开始”菜单选择“开始 > 程序 > Huawei > Policy Center > Uninstall or Delete Components”。但无法显示卸载对话框；
  - 通过IE浏览器访问安全管理器或安全控制器，但无法显示安全管理器或安全控制器的登录页面。
- 修改数据执行保护操作步骤
  - 使用“administrator”账号登录MicrosoftWindowsServer2003操作系统；
  - 选择“开始>设置>控制面板”；
  - 双击“系统”，选择“高级”页签；
  - 在“性能”区域框单击“设置”；
  - 选择“数据执行保护”页签；
  - 选中“只为关键Windows程序和服务启用数据执行保护”；
  - 单击“确定”返回“系统属性”对话框。界面提示需要重新启动操作系统；
  - 单击“确定”退出“系统属性”对话框；
  - 重启MicrosoftWindowsServer2003操作系统，使修改数据执行保护生效。

Policy Center服务器无法正常启动

- 问题描述
  - 服务器启动不成功，一分钟左右定期启动一次。
- 原因分析
  - Policy Center服务器所需端口被其它程序占用，通过netstat–ano|find“port”发现Policy Center服务器所使用端口被哪些程序进程所占用。
- 解决办法
  - 通过“任务管理器”终止被占用端口的程序进程。



- 安全管理器和安全控制器端口列表
  - 1812 802.1x认证端口；
  - 1813 802.1x认证端口；
  - 3288 SACG通信端口；
  - 8080 安全管理器与安全控制器的通信端口；
  - 8443 HTTPS端口；
  - 8005 关闭服务端口；
  - 17889 安全控制器与安全代理通信端口；
  - 21 FTP监听端口。

客户端切换安全控制器引起功能缺失

- 问题描述
  - NAC访问安全控制器A时，NAC客户端功能使用正常，但切换至安全控制器B时，出现功能项缺失问题。
- 原因分析
  - 出现功能项缺失问题可能是由于安装单独的安全控制器过程，选择安全管理器的IP地址填写不正确导致。至安全控制器的服务器上打开C:\ProgramFiles\Policy Center\tomcat\secospace\remote.properties文件查看安全管理器的IP地址的正确性。
- 解决办法
  - 在remote.properties文件内修改安全管理器的IP地址。



- 打开C:\ProgramFiles\Policy Center\tomcat\secospace\remote.properties 后，可以通过记事本程序打开remote.properties文件，在文件内修改seocspace.remote.sm.ip

客户端切换安全控制器引起策略模板异常

- 问题描述
  - 客户端Agent访问安全控制器A时策略模板下发正常，但切换至安全控制器B时，出现策略模板未下发或下发不正常。
- 原因分析
  - 此问题主要是由于安全控制器B与安全管理器或数据库连接存在问题。
- 解决办法
  - 确保安全控制器B与安全管理器或数据库的连通性，若问题还无法定位可重新启动安全控制器B。



- 定位安全控制器B与安全管理器之间的连通性，可通过在安全控制器B上ping管理器的连通性。定位安全控制器B与数据库之间的连通性，可通过在安全控制器B上telnet Database-IP 1433确认连通性。

软件分发不能正常向客户端下载文件

- 问题描述
  - 客户端Agent不能正常从软件分发功能处下载文件。
- 原因分析
  - 此问题主要是由于FTP服务器的安装或配置存在问题。
- 解决办法
  - 按要求完成FTP服务器配置；
  - 解决客户端PC与FTP服务器的IP可达性问题；
  - 解决客户端PC与FTP服务器的防火墙配置问题。



HUAWEI

- FTP服务器安装或配置问题定位：
  - 通过在客户端PC上telnet FTP IP 21测试连通性，然后再到FTP服务器上通过netstat –ano | find “21”确认FTP服务器是否启动；
  - 在客户端PC上使用浏览器访问FTP（如FTP://ftp-IP）， 若不能访问则是FTP服务器配置存在问题。若可访问但无法显示文件页面，基本确定是防火墙把数据通道给阻断（FTP是属于多通道协议），请调整客户端PC或中间防火墙配置。



目录



Vista未安装补丁导致NAC客户端安装失败

- 问题描述
  - 在未安装SP补丁的Microsoft Windows Vista安装NAC客户端，在安装过程中被中断，安装NAC客户端失败。
- 原因分析
  - 该问题为Microsoft Windows Vista操作系统本身的问题，由于未安装SP补丁引起NAC客户端安装程序被阻塞，导致NAC客户端安装失败。
- 解决办法
  - 先安装Microsoft Windows Vista SP1补丁，再安装NAC客户端即可解决问题。



- 先从微软官方网站获取Microsoft Windows Vista SP1补丁，然后再安装补丁文件，最后安装NAC客户端。

缺少写权限导致NAC客户端安装失败

- 问题描述
  - 在一台终端主机运行NAC客户端安装程序，安装完成后发现“开始”菜单缺少NAC客户端的快捷方式。



- 原因分析
  - 在运行NAC客户端时，安装程序会先把程序释放到预设的目录，如果安装程序对该目录没有写权限，则会导致安装会失败。
- 解决办法
  - 安装程序预留接口，通过增加注册表键值，以便手工将释放目录调整为具有写权限的操作系统临时目录。最后重新运行安装程序即可解决问题。



- 解决步骤
  - 在Microsoft Windows操作系统选择“开始>运行”，输入“regedit”后按“Enter”；
  - 在“HKEY_LOCAL_MACHINE\SOFTWARE”添加类型为“字符串”，名称为“CHANGE_TEMP”，取值为“true”的键；
  - 重新运行NAC客户端安装程序。



- 问题描述
  - 在Microsoft Windows操作系统上尝试安装NAC客户端，发现NAC客户端只能安装在C盘，但无法安装在D盘。
- 原因分析
  - Administrators组和System账号缺少D盘的访问权限。
- 解决办法
  - 在D盘为Administrators用户组和System账号的授予完全控制权限即可。





- 解决步骤
  - 使用“administrator”账号登录MicrosoftWindows。打开资源管理器。右键单击D盘，选择“共享与安全”。选择“安全”页签；
  - 单击“高级”，选择“所有者”，选中“Administrator”和“替换子容器及对象的所有者”；
  - 右键单击D盘，选择“共享与安全”和“安全”页签。单击“添加”，输入Administrators，然后选中“完全控制”，单击“应用”；
  - 单击“添加”，输入System，单击“确定”，然后选中“完全控制”，单击“应用”；
  - 重新安装NAC客户端

NAC客户端在安装过程中掉电导致终端主机启动缓慢

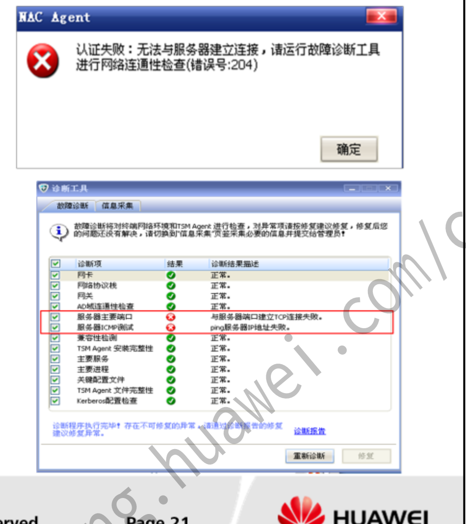
- 问题描述
  - 在一台安装Microsoft Windows Vista操作系统上安装NAC客户端时，突然断电或者被主动防御类软件（例如安全卫士360）拦截导致安装过程异常终止。在重新启动Microsoft Windows Vista时发现启动过程很缓慢，大约花费10min才完成启动。
- 原因分析
  - NAC客户端安装过程中会安装NDIS网络驱动。而Microsoft Windows Vista在NDIS驱动安装功能上存在缺陷，如果该驱动安装失败可能导致操作系统启动缓慢的问题。
- 解决办法
  - 重新启动计算机并按“F8”选安全模式进入操作系统，运NAC客户端安装程序。



- 运行NAC客户端的安装程序，NAC客户端安装程序会自动清理安装残留信息。残留信息清理完成后会提示重新启动计算机。
- 重新启动计算机，并以正常模式登录，最后安装NAC客户端即可解决问题。



- 问题描述
  - NAC客户端认证提示“认证失败：无法与服务器建立连接，请运行故障诊断工具进行网络连通性检查”。
- 原因分析
  - 服务器地址设置错误。
  - 终端主机与服务器之间的网络不可达。
- 解决办法
  - 检查客户端设置服务器地址的正确性；
  - 运行NAC客户端故障诊断工具，检查终端主机与服务器的网络连通性。根据诊断结果与修复建议，进行网络修复。



HUAWEI

- 检查客户端所设置的服务器IP地址的正确性：在NAC客户端界面的右上方单击“认证”，在认证窗口的左下角单击“高级设置”，在“服务器”栏检查Policy Center服务器的IP地址是否正确（可能显示的不是IP地址而是归属地名称）。或可以通过c:\netstat – ano检查TCP协议状态是17889的IP地址。
- 运行NAC客户端故障诊断工具： “服务器主要端口”和“服务器ICMP测试”将会同时提示失败。服务器主要端口”显示“与服务器端口建立TCP连接失败”，而“服务器ICMP测试”将显示“ping服务器IP地址失败”。
- 针对“服务器ICMP测试”将给出修复建议如下：
  - 请检查服务器IP地址是否配置正确；
  - 请检查终端与服务器路由是否可达。
- 针对“服务器主要端口”将给出修复建议如下：
  - 请检查服务器IP地址是否配置正确；
  - 请检查终端与服务器路由/端口是否可达；
  - 请联系管理员检查Policy Center服务器是否正常运行



- 问题描述
  - NAC客户端认证提示“网络访问受限，请联系管理员处理”。
- 原因分析
  - 由于Policy Center服务器管理页面上未将出现此问题的终端IP地址，加入到SACG配置页面的客户端地址池中。
- 解决办法
  - 在Policy Center服务器管理页面上将出现问题终端的IP地址（段）加入到SACG配置的地址池中，点击“同步硬件SACG”。





- 通过在Policy Center产品文档搜索1501定位问题原因为，终端IP地址未加入到SACG配置页面的客户端地址池中。通过查看硬件SACG配置界面未显示终端IP地址段信息配置、或通过信息搜集工具查询Agent.log文件提示“2011-12-0916:45:11认证管理[02011]:没有找到SACG信息，该终端地址不在SACG地址池中”，或通过dis right-manager online-users未发现任何此认证终端信息。通过在Policy Center服务器（SM）管理页面上将出现问题终端的IP地址（段）加入到SACG配置的地址池中，点击“同步硬件SACG”，终端重新认证即成功。

WebAgent认证界面无法显示

- 问题描述
  - 使用WebAgent进行客户端认证，发现认证界面一直无法显示。
- 原因分析
  - 由于终端IE浏览器设置安全级别过高，导致webagent的ActiveX插件无法安装成功，无法进行认证。
- 解决办法
  - 至IE浏览器安全设置将“对标记为可安全执行脚本的ActiveX控件执行脚本”、“下载未签名的ActiveX控件”和“运行ActiveX控件和插件”设置为“启用”。



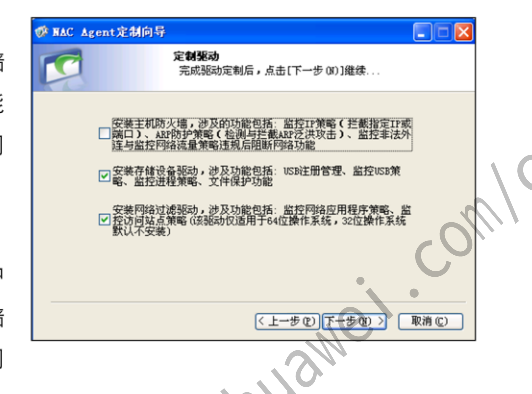


- 解决步骤：
  - 在IE浏览器顶端的工具栏中选择“工具>Internet选项”。
  - 单击“安全”页签，选择“Internet”，单击“自定义级别”。
  - 将“对标记为可安全执行脚本的ActiveX控件执行脚本”、“下载未签名的ActiveX控件”和“运行ActiveX控件和插件”设置为“启用”，单击“确定”。
  - 界面提示“是否要更改该区域框的安全设置”。
  - 单击“是”。
  - 单击“确定”。



安装NAC客户端后无法访问网页

- 问题描述
  - 安装NAC客户端后无法对网页进行访问浏览。
- 原因分析
  - 由于NAC客户端具有软件主机防火墙模块，存在与其他具有防火墙功能软件冲突的可能，导致无法访问网页问题。
- 解决办法
  - 对已经安装了软件主机防火墙客户端，可对其分发不包含主机防火墙功能的策略（如监控网址、监控网络应用程序、非法外联等）。



HUAWEI

- 解决方法：Policy Center提供客户端主机防火墙动态加载功能，可以将对应的客户端分配不包含主机防火墙功能的策略（如监控网址、监控网络应用程序、非法外联等）；若对应客户端一定需要使用相关策略，可以建议将冲突软件卸载或者关闭其防火墙模块

NAC客户端定期重新认证

- 问题描述
  - NAC客户端每隔几分钟就进行重新认证。
- 原因分析
  - 由于NAC客户端后台服务程序Secodaemon.exe被第三方主动防御软件终止，
  - 而由NAC客户端后台保护程序将此exe进程重新启动，如此循环导致重复认证和上线。
- 解决办法
  - 在第三方防御软件上把NAC客户端加入至可信列表中。

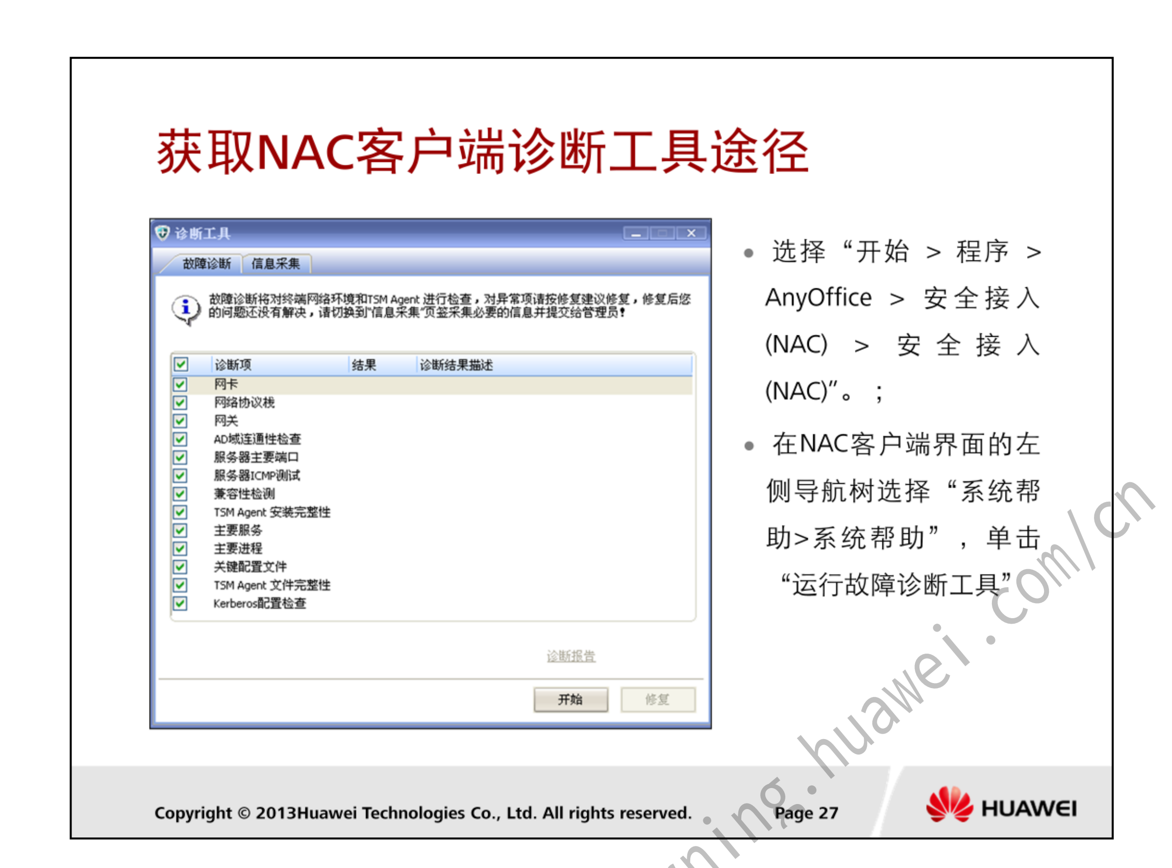


- 解决方法：安装NAC客户端时，将第三方主动防御软件的提示（如360安全卫士提示的一些注册表写入，服务安装等），点击“允许”或者将NAC客户端主进程Secodaemon.exe加入到信任程序列表中即可。

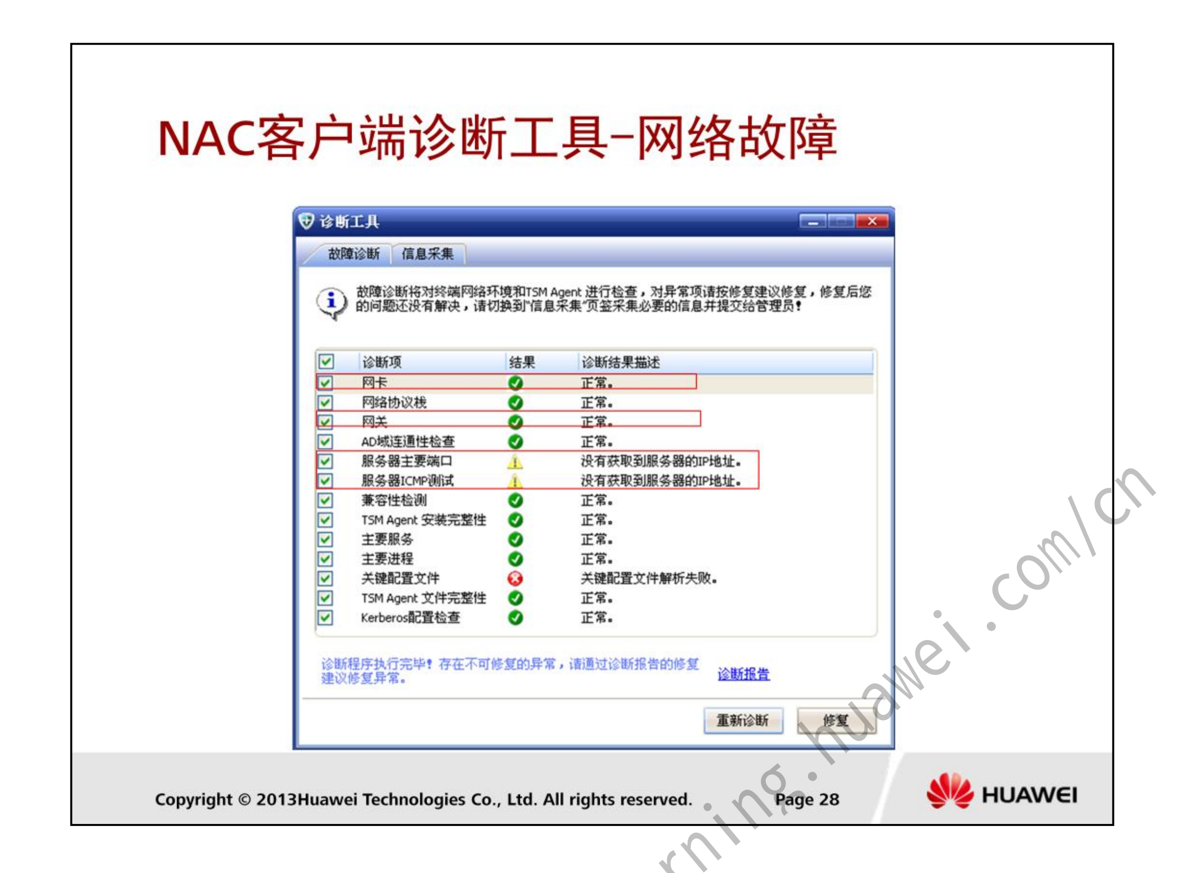


目录





- 当NAC客户端出现故障时，使用NAC客户端诊断工具对NAC客户端的常见诊断选项进行检测，方便终端用户进行初步故障定位。NAC客户端诊断工具是NAC客户端的一个组成部分，在安装NAC客户端时会同时安装NAC客户端诊断工具。



- 网卡诊断：检测网卡物理链路状态，即网线是否松脱，网卡是否成功获取IP地址、网卡是否被禁用；
- 网关诊断：检测终端主机与网关在二层物理链路的连通性；
- 服务器主要端口诊断：检测服务器的TCP端口17889是否可达；
- 服务器ICMP测试诊断：检测终端主机与服务器之间链路连通性。

NAC客户端诊断工具-自动修复

诊断工具

故障诊断 信息采集

故障诊断将对终端网络环境和TSM Agent 进行检查，对异常项请按修复建议修复，修复后您的问题还没有解决，请切换到"信息采集"页签采集必要的信息并提交给管理员！

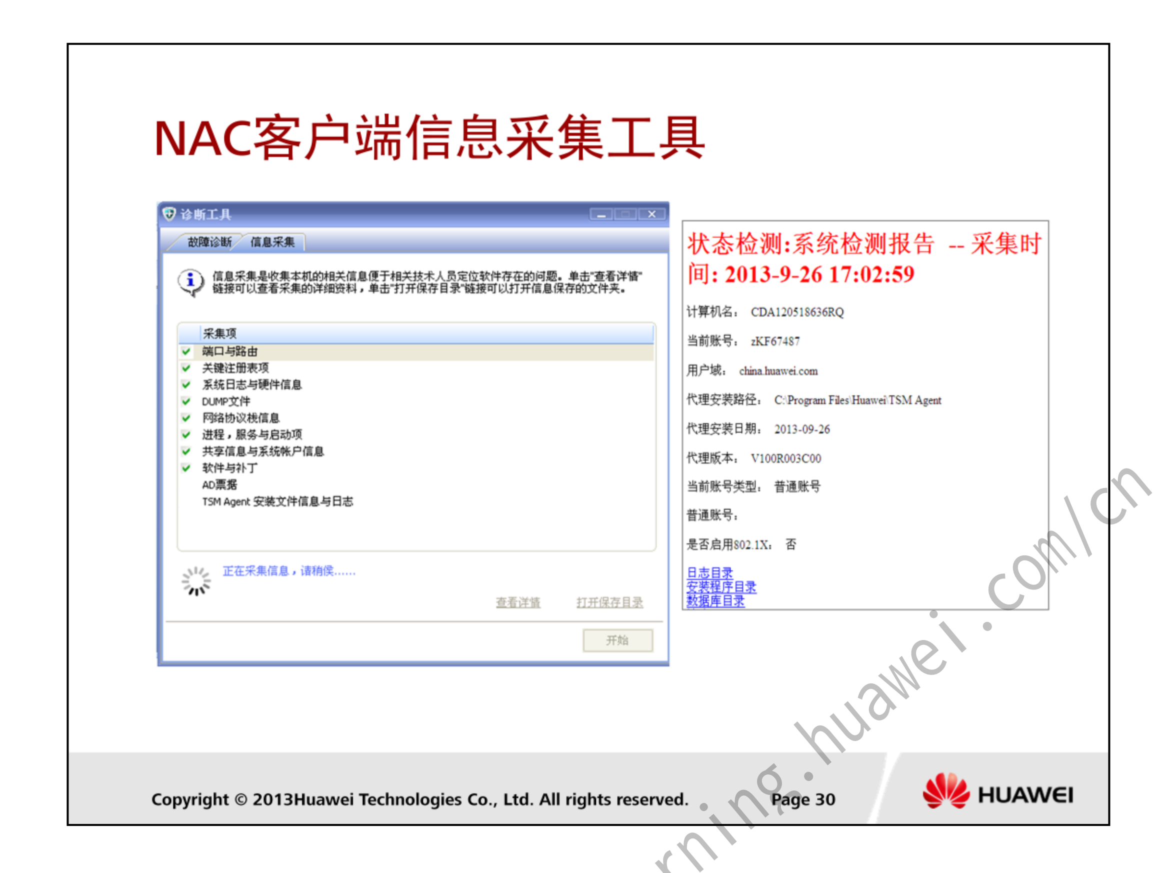
诊断项	结果	诊断结果描述
网卡	✔	正常。
网络协议栈	✔	正常。
网关	✔	正常。
AD域连通性检查	✔	正常。
服务器主要端口	⚠	没有获取到服务器的IP地址。
服务器ICMP测试	⚠	没有获取到服务器的IP地址。
兼容性检测	✔	正常。
TSM Agent 安装完整性	✔	正常。
主要服务	✔	正常。
主要进程	✔	正常。
关键配置文件	✖	关键配置文件解析失败。
TSM Agent 文件完整性	✔	正常。
Kerberos配置检查	✔	正常。

诊断程序执行完毕！存在不可修复的异常，请通过诊断报告的修复建议修复异常。 诊断报告

重新诊断 修复

HUAWEI

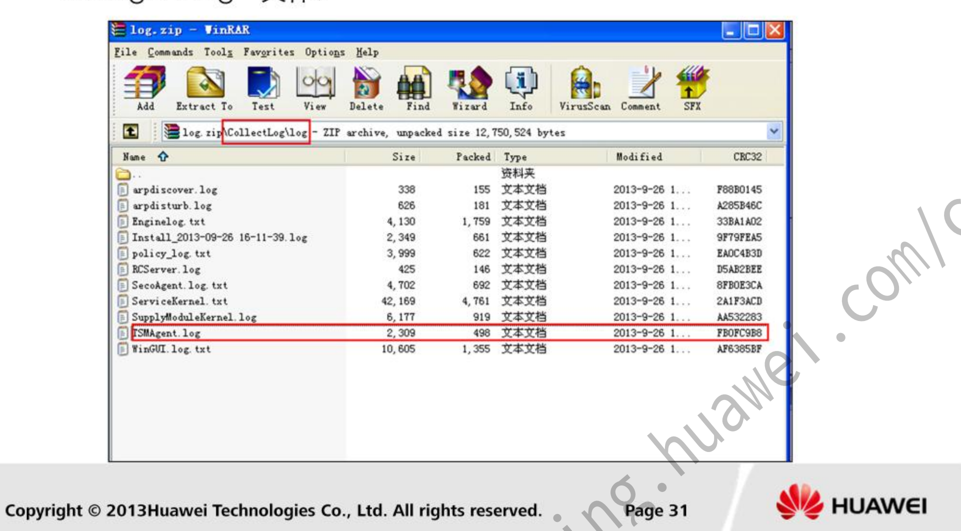
- 自动修复是指当NAC客户端出现故障时，NAC客户端诊断工具通过修复网络协议栈异常、修复启动进程和后台服务、修复关键配置文件来尝试修复故障。
  - 网络协议栈自动修复：如果发现网络协议栈出现异常，NAC客户端诊断工具将会自动重新初始化网络协议栈；
  - 后台服务自动修复：如果发现NAC客户端的后台服务处于停止状态，NAC客户端诊断工具将会自动启动下面的后台服务，SecoDaemon服务、SecoVNC服务、USBFILT服务；
  - 进程自动修复：如果发现NAC客户端的进程处于停止状态，NAC客户端诊断工具将会自动启动“WinGUI”进程；
  - 关键配置文件自动修复：当发现关键配置文件被损坏，NAC客户端诊断工具把配置文件恢复到安装时的状态。



- 当故障诊断和自动修复均无法解决问题时，可通过NAC客户端信息采集工具搜集NAC客户端与故障相关的信息提交给研发专家进行故障定位。
- 操作步骤：
  - 在“诊断工具”界面选择“信息采集”页签；
  - 单击“开始”，选择采集结果的存放路径；
  - 选择采集结果的存放位置后，开始采集故障信息；
  - 单击“查看详情”，查看详细的信息采集结果或把“log.zip”提交给研发专家帮助定位故障。

定位采集信息文件

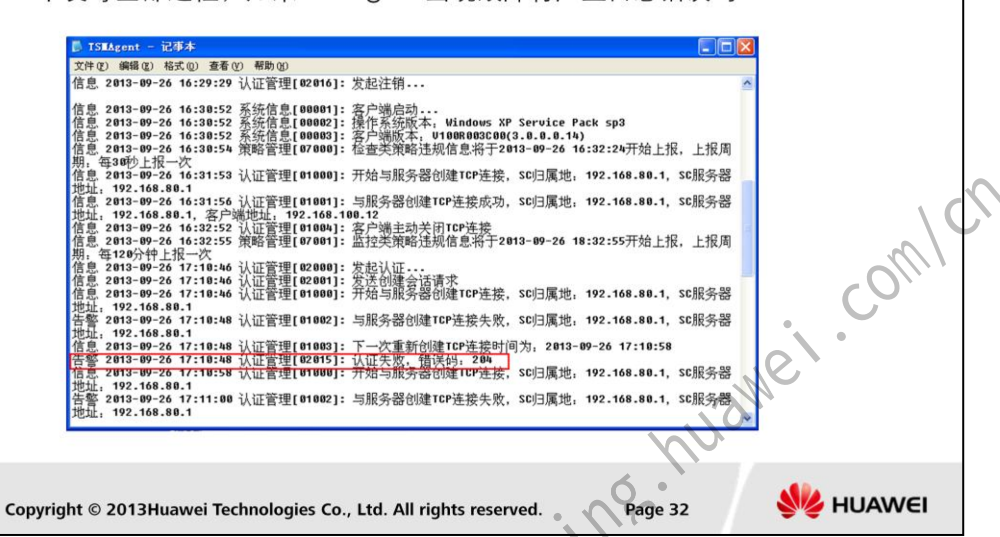
- 将采集的log压缩文件解压，找到“log>CollectLog>log”路径下的“TSMAgent.log”文件。



- 对于通过远程信息采集工具或终端故障诊断工具采集上来的信息，我们可以通过查看LOG日志进行初步的问题定位。

定位NAC客户端采集信息错误码

- 打开“TSMAgent.log”文件，从log日志中可看到agent认证、安全策略下发等全部过程，如果TSMAgent出现故障将产生日志错误码。


TSMAgent - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
信息 2013-09-26 16:29:29 认证管理[02016]: 发起注销...

信息 2013-09-26 16:30:52 系统信息[00001]: 客户端启动...
信息 2013-09-26 16:30:52 系统信息[00002]: 操作系统版本: Windows XP Service Pack sp3
信息 2013-09-26 16:30:52 系统信息[00003]: 客户端版本: V100R003C00(3.0.0.0.14)
信息 2013-09-26 16:30:54 策略管理[07000]: 检查类策略违规信息将于2013-09-26 16:32:24开始上报, 上报周期: 每30秒上报一次
信息 2013-09-26 16:31:53 认证管理[01000]: 开始与服务器创建TCP连接, SC归属地: 192.168.80.1, SC服务器地址: 192.168.80.1
信息 2013-09-26 16:31:56 认证管理[01001]: 与服务器创建TCP连接成功, SC归属地: 192.168.80.1, SC服务器地址: 192.168.80.1, 客户端地址: 192.168.100.12
信息 2013-09-26 16:32:52 认证管理[01004]: 客户端主动关闭TCP连接
信息 2013-09-26 16:32:55 策略管理[07001]: 监控类策略违规信息将于2013-09-26 18:32:55开始上报, 上报周期: 每120分钟上报一次
信息 2013-09-26 17:10:46 认证管理[02000]: 发起认证...
信息 2013-09-26 17:10:46 认证管理[02001]: 发送创建会话请求
信息 2013-09-26 17:10:46 认证管理[01000]: 开始与服务器创建TCP连接, SC归属地: 192.168.80.1, SC服务器地址: 192.168.80.1
告警 2013-09-26 17:10:48 认证管理[01002]: 与服务器创建TCP连接失败, SC归属地: 192.168.80.1, SC服务器地址: 192.168.80.1
信息 2013-09-26 17:10:48 认证管理[01003]: 下一次重新创建TCP连接时间为: 2013-09-26 17:10:58
告警 2013-09-26 17:10:48 认证管理[02015]: 认证失败, 错误码: 204
信息 2013-09-26 17:10:58 认证管理[01000]: 开始与服务器创建TCP连接, SC归属地: 192.168.80.1, SC服务器地址: 192.168.80.1
告警 2013-09-26 17:11:00 认证管理[01002]: 与服务器创建TCP连接失败, SC归属地: 192.168.80.1, SC服务器地址: 192.168.80.1
```


- 打开“TSMAgent.log”文件，从log日志中可看到agent认证、安全策略以及错误代码，有了错误代码之后就可以做下一步的操作。

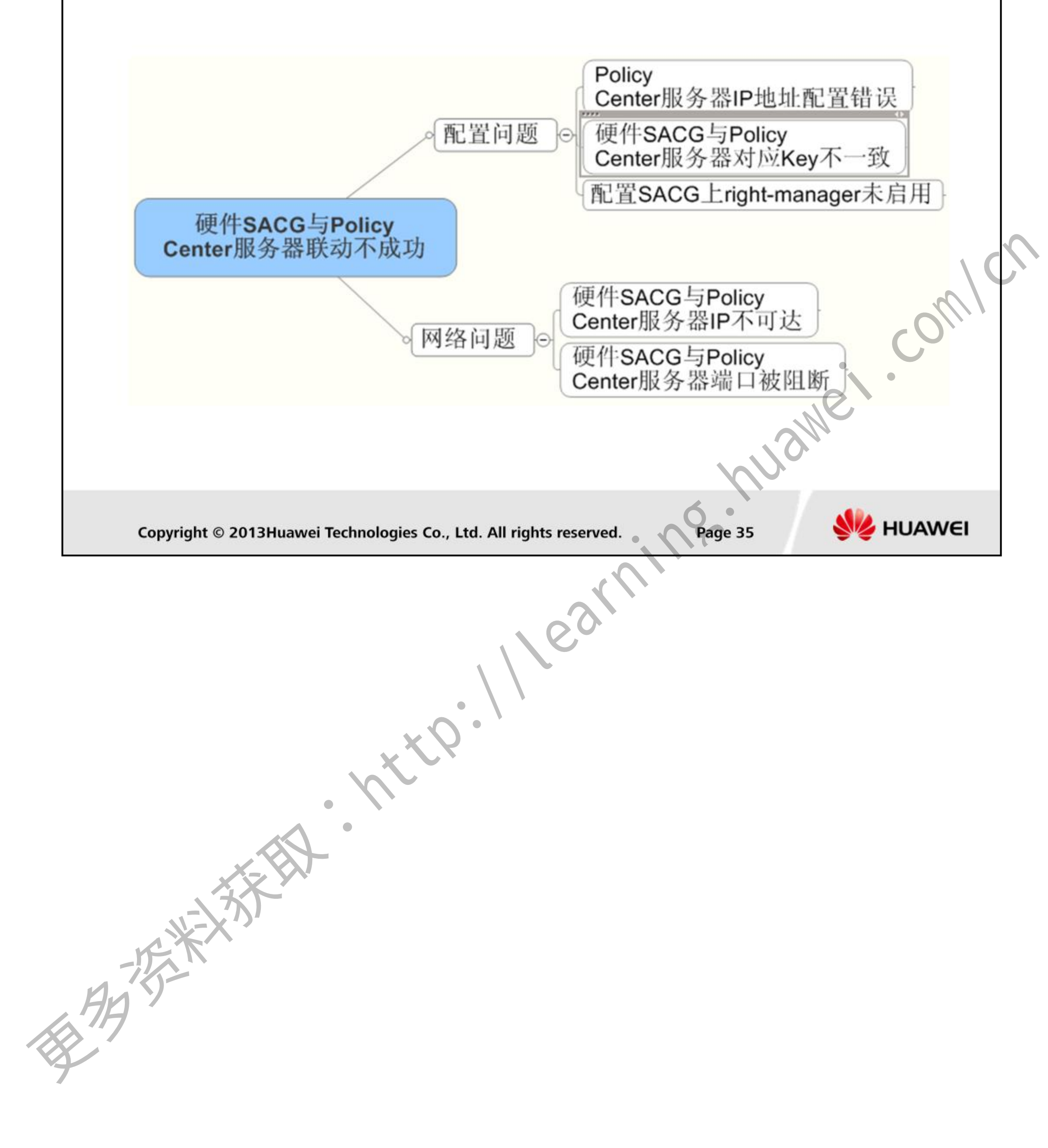


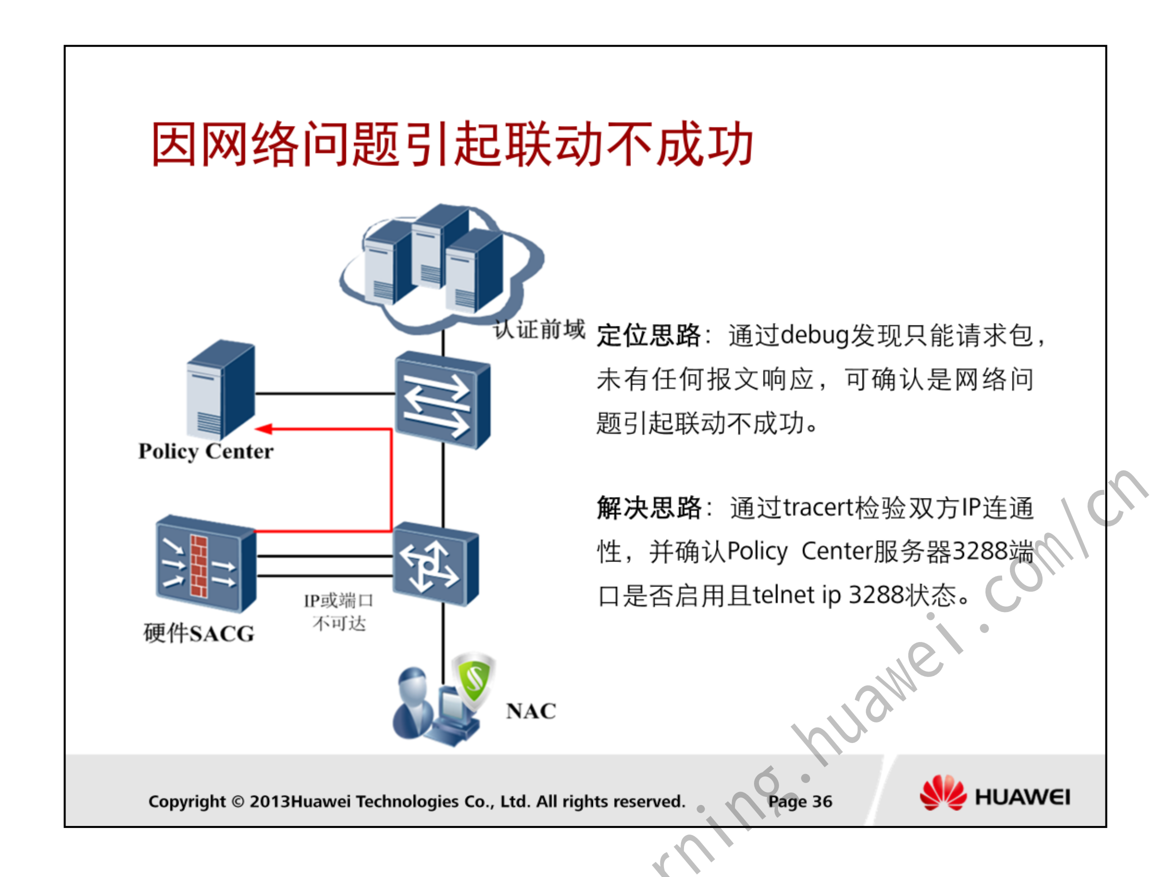
- 在NAC客户端界面左侧导航树选择“系统帮助>系统帮助”，单击“打开联机帮助”；
- 在搜索栏中输入log中给出的错误码，就可以看到该故障的原因及解决办法



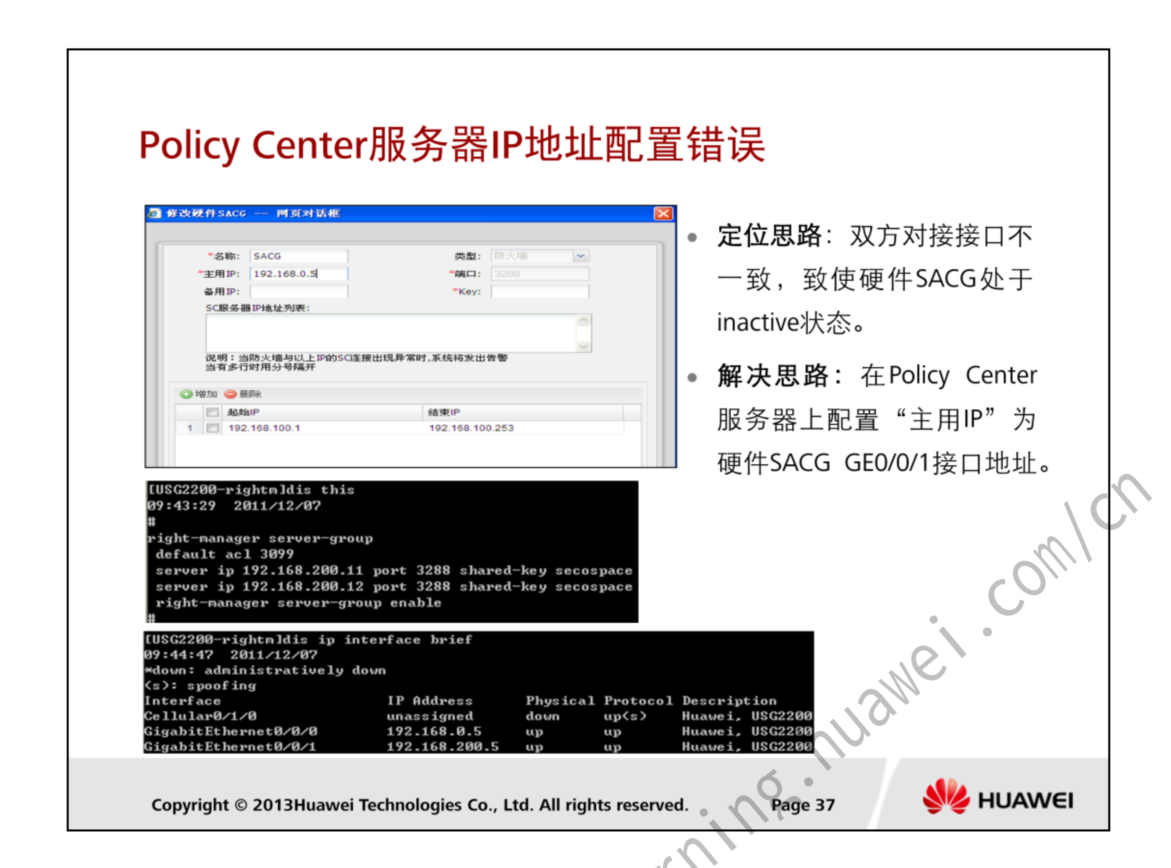
目录




案例一：SACG与Policy Center服务器联动不成功
硬件SACG与Policy Center服务器联动不成功
配置问题
Policy Center服务器IP地址配置错误
硬件SACG与Policy Center服务器对应Key不一致
配置SACG上right-manager未启用
网络问题
硬件SACG与Policy Center服务器IP不可达
硬件SACG与Policy Center服务器端口被阻断
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 35
HUAWEI

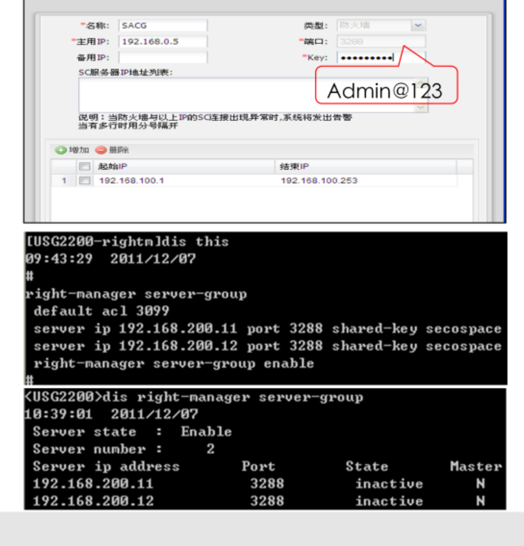


- 采用debugging right-manager all后显示如下信息
  0.4642700SACG%%01SACG/8/debug(d):EVENTfromCOPSmoduleconnectto192.168.200.11（policy Center 地址）
  0.4647700SACG%%01SACG/8/debug(d):EVENTfromCOPSmoduleconnectto192.168.200.11
- 检查Policy Center服务器的服务端口是否已处于listening状态：C:\netstat –ano | find “3288”；
- 通过ping和tracert确认硬件SACG与Policy Center服务器之间IP连通性；
- 通过telnet192.168.200.113288确认硬件SACG与Policy Center服务器之间端口连通性；
  - IP与端口未被阻断；
    <USG2200>telnet192.168.200.11 445
    15:25:212011/12/07
    Trying192.168.200.11...
    PressCTRL+Ttoabort
    Connected to 192.168.200.11...
    The connection was closed by the remote host!
  - IP或端口已被阻断，或Policy Center服务器的服务端口3288未启用。
    <USG2200>telnet192.168.200.11 3288
    15:25:292011/12/07
    Trying192.168.200.11...
    PressCTRL+Ttoabort
    Can ‘tconnecttotheremotehost!



- 通过以上图示可以看出，硬件SACG是通过G0/0/1与SC控制器通讯，而SC控制器却与硬件SACG的G/0/0进行通讯，由于双方进行交互的接口不对应，致使硬件SACG一直处于inactive状态（可执行display right-manager server-group命令查看）。
- 通过变更Policy Center服务器“主用IP”为硬件SACG G0/0/1 IP地址，同步硬件SACG后硬件SACG的状态变为active。

双方key不一致



- **定位思路**：硬件SACG与Policy Center服务器之间有数据包交互，但连接总被closed掉。那么基本定位为双方key不一致。
- **解决思路**：检查双方key配置，注意空格和大小写。



- 通过以上图示可以看出，硬件SACG与Policy Center控制器之间通讯或配置存在问题，采用debugging right-manager all后显示如下信息(双方连接总是被closed，那么基本可确认是双方key配置不一致引起)：

  0.10890800SACG%%01SACG/8/debug(d):EVENTfromCOPSmoduleconnectto 192.168.200.11.

  0.10890900SACG%%01SACG/8/debug(d):EVENTfromCOPSmoduleconnectto 192.168.200.11ok.

  0.10891016SACG%%01SACG/8/debug(d):PACKETfromCOPSmodulesendapacket,length:24,byconnid:0,nowsended24

  0.10891150SACG%%01SACG/8/debug(d):PACKETfromCOPSmodulereceive8

  0.10891233SACG%%01SACG/8/debug(d):PACKETfromCOPSmodulereceive8

  0.10891316SACG%%01SACG/8/debug(d):PACKETfromCOPSmodulereceive0

  0.10891400SACG%%01SACG/8/debug(d):PACKETfromCOPSmoduleCopsPacketDemarcate16

  0.10891500SACG%%01SACG/8/debug(d):PACKETfromCOPSmodulepPacket:acf555cLen:10ConId:0

  0.10891616SACG%%01SACG/8/debug(d):EVENTfromCOPSmoduleconnid:0closed

right-manager功能未启用

```
<USG2200>debugging right-manager event
11:22:20  2011/12/07
right-manager server-group
 default acl 3099
 server ip 192.168.200.11 port 3288 shared-key secospace
 server ip 192.168.200.12 port 3288 shared-key secospace
#
<USG2200>dis right-manager server-group
10:39:01  2011/12/07
 Server state  :  Enable
 Server number :      2
 Server ip address          Port          State        Master
 192.168.200.11              3288           inactive       N
 192.168.200.12              3288           inactive       N
```

- 定位思路：通过debug和查看right-manager server-group命令，未发生任何输出信息和配置。
- 解决思路：debugright-managerevent未发生任何debug信息输出，可确认是Right-manager未启用导致。



- 通过以上图示可以看出，是由于right-manager未启用导致硬件SACG与Policy Center控制器之间连接不能正常建立。且通过debug right-manager event未有任何debug信息输出，可确认是Right-manager未启用导致。通过配置right-manager server-group enable命令后，right-manager server-group状态信息将变为active。

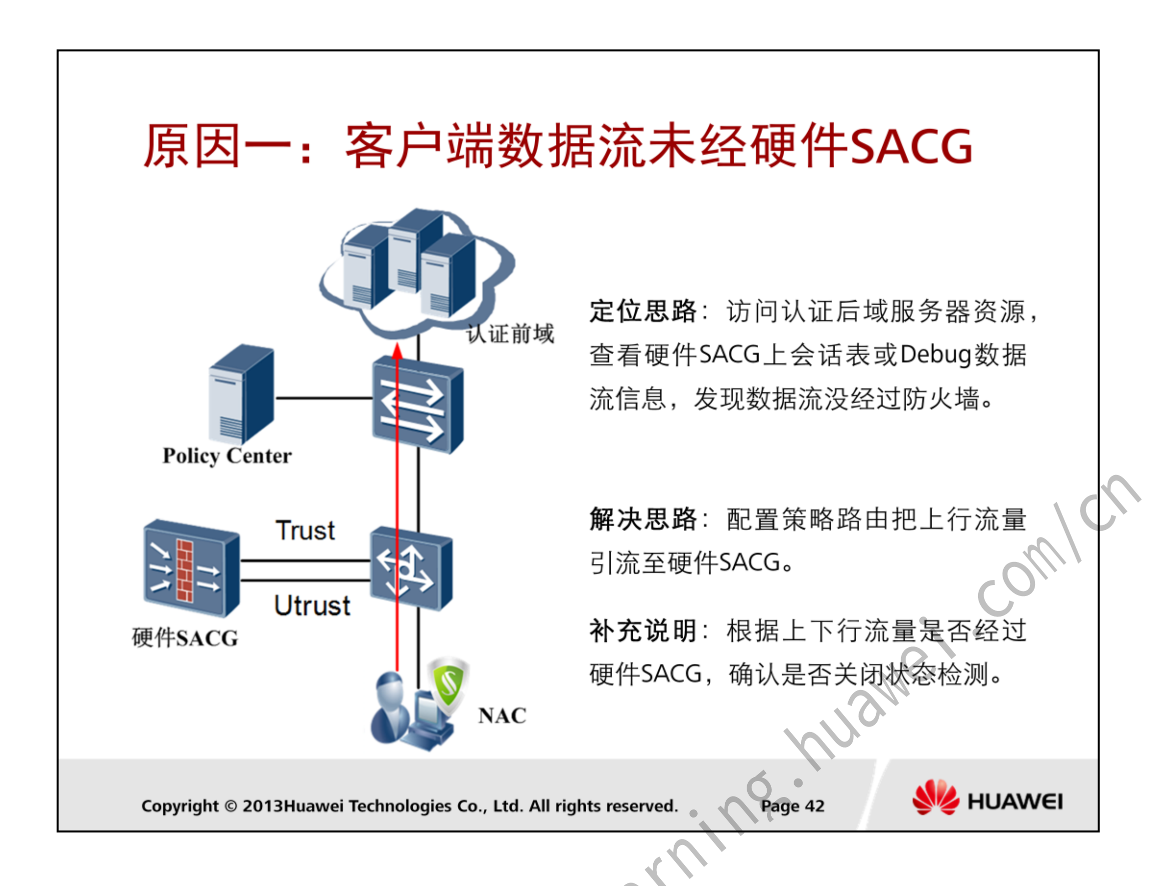
SACG与Policy Center服务器数据包交互

debuggingright-managerall关键提示

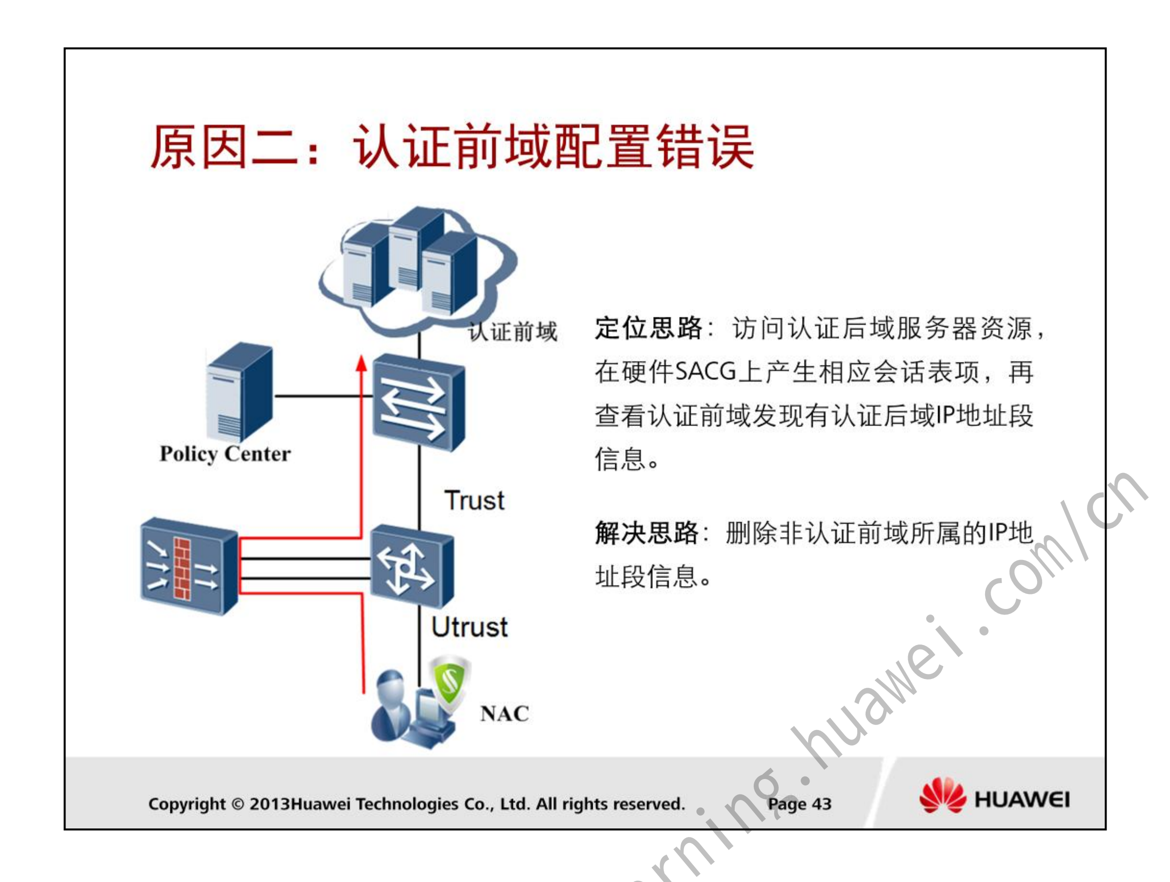
提示	含义
EVENTfromCOPSmoduleconnectto192.168.20.10ok.	SACG可以连接到Policy Center服务器的3288端口
PACKETfromCOPSmodulesendapacket,length:24,byconnid:0,nowsended24PACKETfromCOPSmodulereceive 8	SACG与Policy Center服务器互有收发
EVENTfromMAINmodulesacgrcvmsg:copstype=RIGHTM_COPSMSG_CONNOK EVENTfromMAINmodulesacgsndmsg:copstype=COPS_FAI_MSG_REQ_STARTUP	SACG与Policy Center服务器连接建立，开始交互
EVENTfromMAINmoduleSuccess:Serveractive.	SACG与Policy Center服务器联动成功

- 以上为硬件SACG与Policy Center服务器之间正常的数据包交互信息。

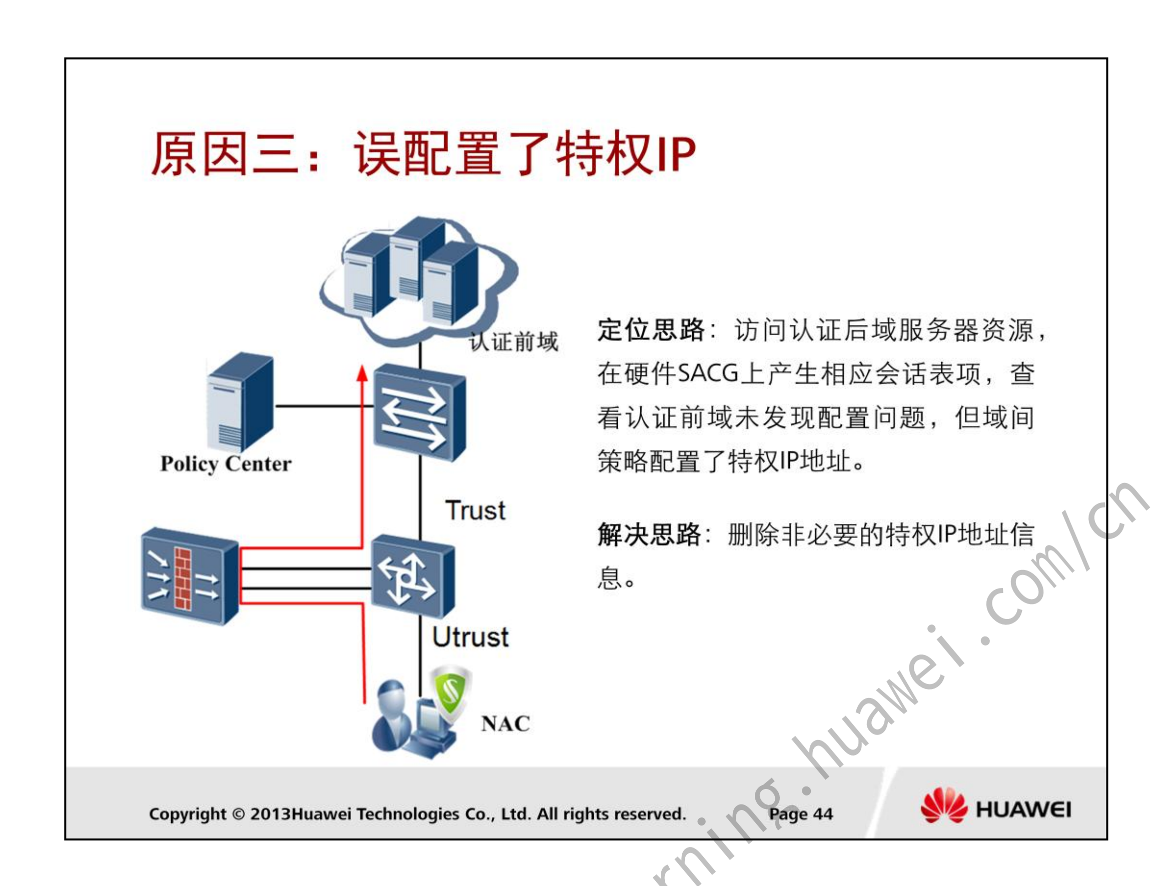

案例二：未认证可访问认证后域资源
问题二：客户端未认证可访问认证后域资源
配置问题
客户端数据流未经过硬件SACG
认证前域配置错误
误配置了特权IP
开启默认域间包过滤
最小存活数量配置错误，激活逃生通道
网络问题
原访问认证后域会话未老化
网络连通性问题，激活逃生通道
Copyright © 2013Huawei Technologies Co., Ltd. All rights reserved.
Page 41
HUAWEI



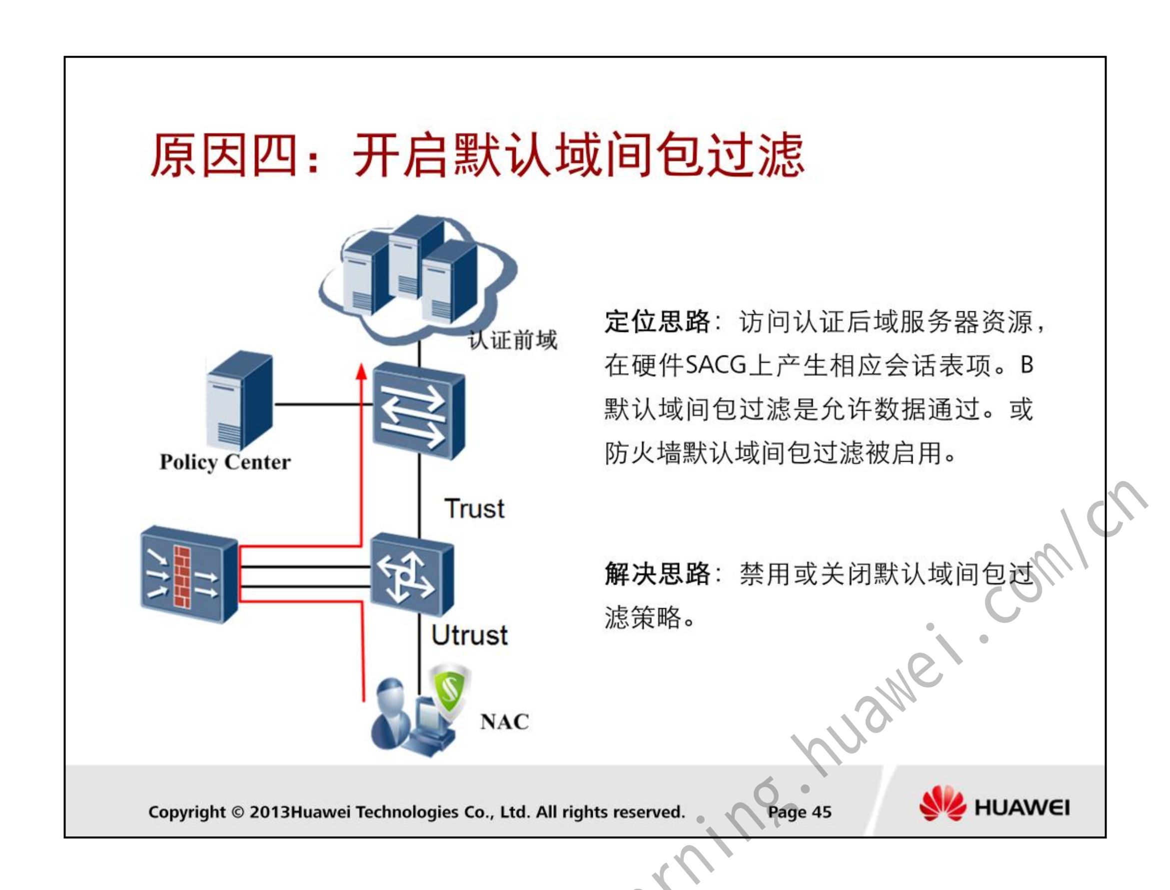
- 查看硬件SACG会话表命令：display firewall session table，未发现客户端访问认证后域服务器资源的会话表信息，或通过debugging tcp packet remote-port 80，再访问Web服务器发现无任何debug信息显示，基本可定位客户端数据流未经过硬件SACG所制。
- 通过策略路由把上行流量引流至硬件SACG，且关闭硬件SACG状态检测后问题解决



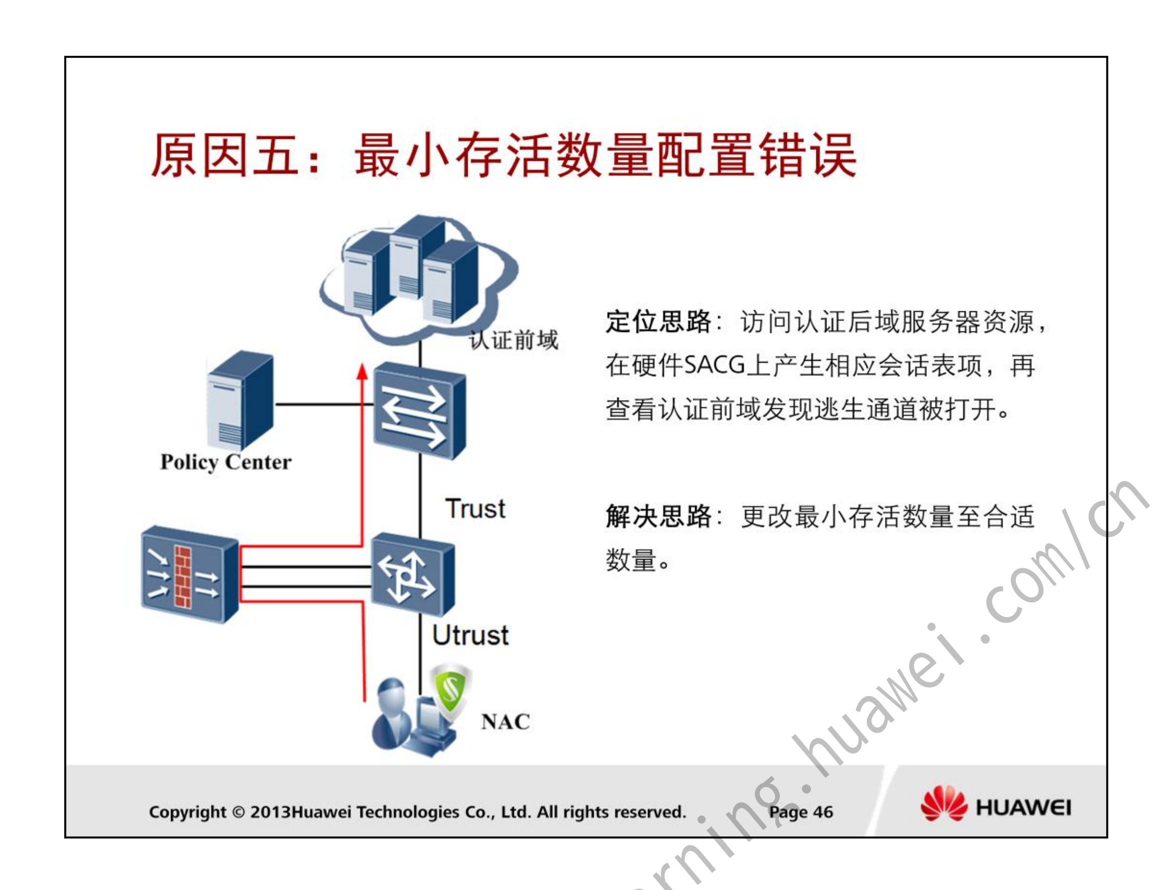
- 查看硬件SACG认证前域命令：display right-manager role-id 0 rule，发现认证前域包含有认证后域IP地址段信息，至Policy Center管理器操作步骤如下：
  - 在管理器的导航栏单击“接入控制”；
  - 在左侧菜单栏选择“接入控制配置>硬件SACG”；
  - 选择“前域”页签，删除不属于认证前域的IP地址段信息；
  - 选择“硬件SACG”页签，单击“同步硬件SACG”进行认证前域的IP地址段信息同步。这时登录防火墙通过display right-manager role-id 0 rule命令发现此次只有认证前域IP地址段信息。



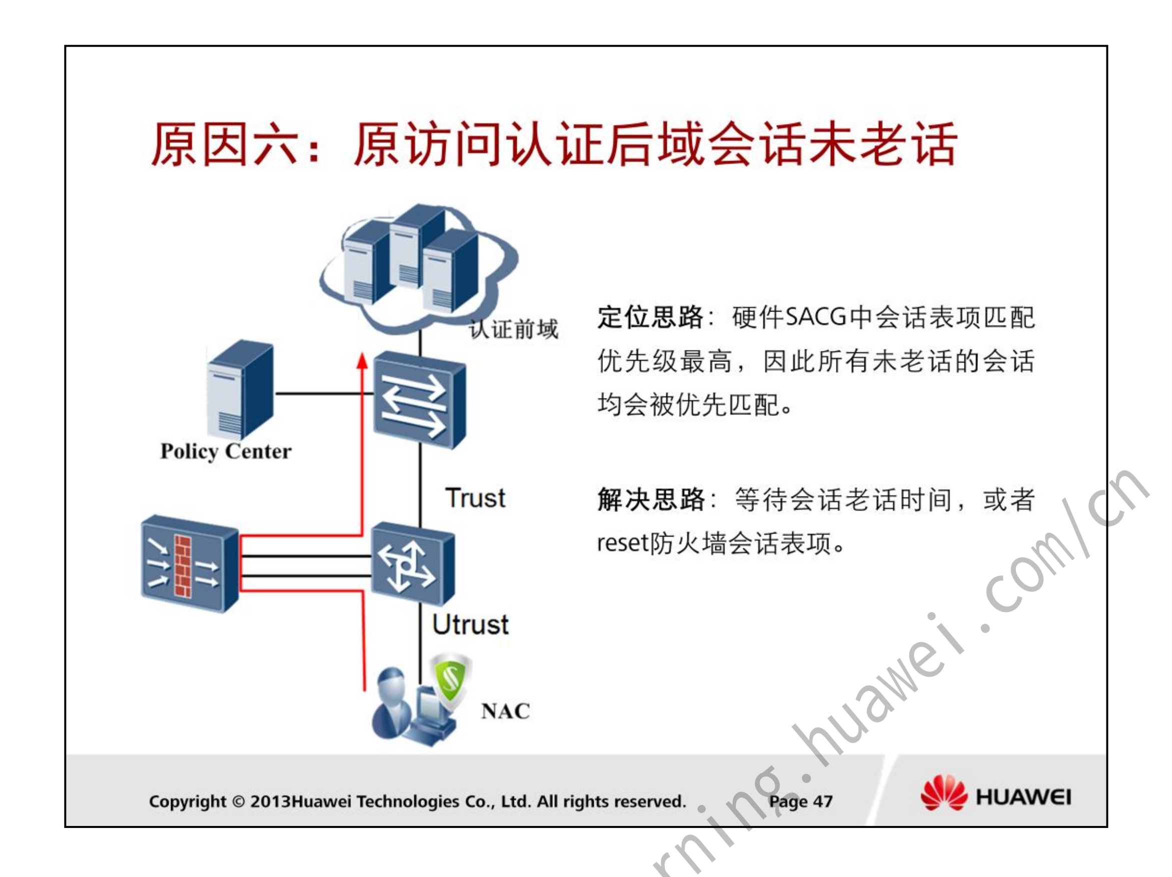
- 查看硬件SACG域间包过滤策略命令：display policy interzone trust untrust inbound，发现有非必要的特权IP地址信息，至硬件SACG undo非必要的特权IP地址信息



- 查看硬件SACG默认域间包过滤策略命令：display firewall packet-filter default all，发现trust与untrust默认安全域间的策略为permit，禁用默认域间包过滤策略（firewall packet-filter default deny interzone trust untrust direction inbound），或关闭默认域间包过滤策略（undo firewall packet-filter default interzone trust untrust direction inbound）。



- 查看硬件SACG认证前域命令：display right-manager role-id 0 rule，发现认证前域中逃生通道被打开，更改最小存活数量至合适数量。比如有20000个以下终端，而部署了3台SC服务器，则应该这样配置最小存活数量：right-manager server-group active-minimum 2，且启用right-manager status-detect enable使用逃生通道功能生效。



- 执行硬件SACG详细的会话表项命令：Dis firewall session table verbose source global X.X.X.X，查看当前会话表项剩余的时间。如以下显示（默认会话生存时间为10分钟，目前还剩余5分27秒）：

  tcpVPN:public-->public

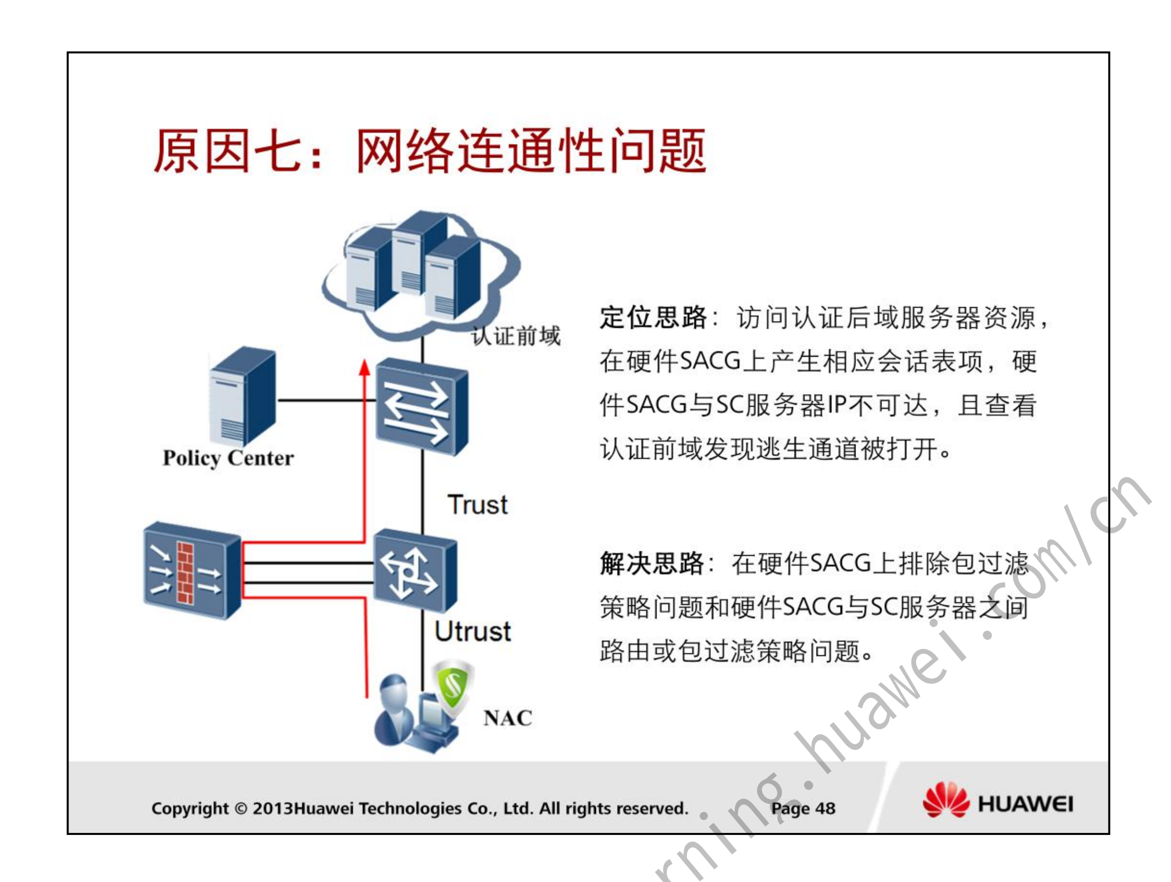
  Zone:untrust-->trustTTL:00:10:00Left:00:05:27

  Interface:GigabitEthernet0/0/1NextHop:192.168.200.11MAC:00-0c-29-d4-47-d2

  <--packets:31bytes:9516-->packets:33bytes:17277

  192.168.0.119:1574-->192.168.200.11:8443

- 或者通过执行reset会话表项（reset firewall session table source global 192.168.0.119）而立即生效。



- 查看硬件SACG会话表命令：display firewall session table，发现客户端访问认证后域服务器资源的会话表信息，但通过在硬件SACG上pingSC服务器发现IP不可达。因此网络连通性问题只可能由以下几类原因组成：
    - 硬件SACG上包过滤策略，导致硬件SACG与SC服务器之间交互报文被硬件SACG过滤掉；
    - 硬件SACG与SC服务器之间无可达路由引起，可通过tracert命令过位问题；
    - 硬件SACG与SC服务器之间有包过滤设备把他们之间的交互的报文过滤掉。



- 客户端已在认证后域或访问认证前域资源是不支持Web推送页面功能。

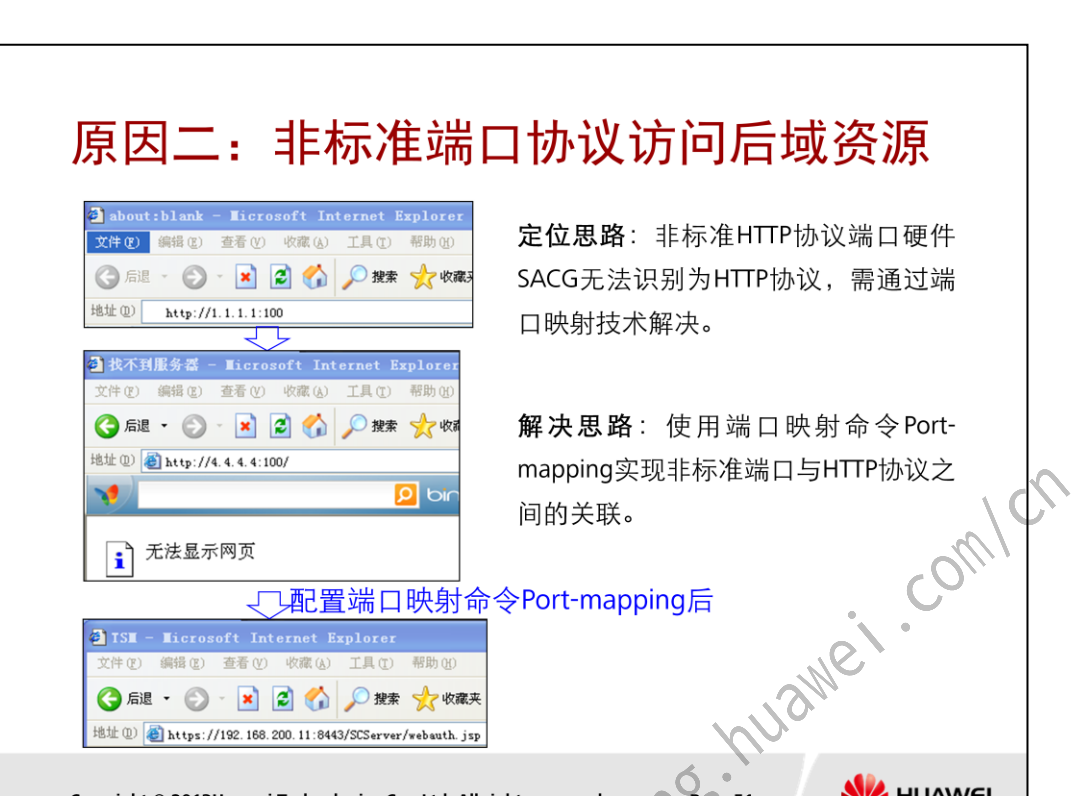
原因一：输入非HTTP协议访问后域资源



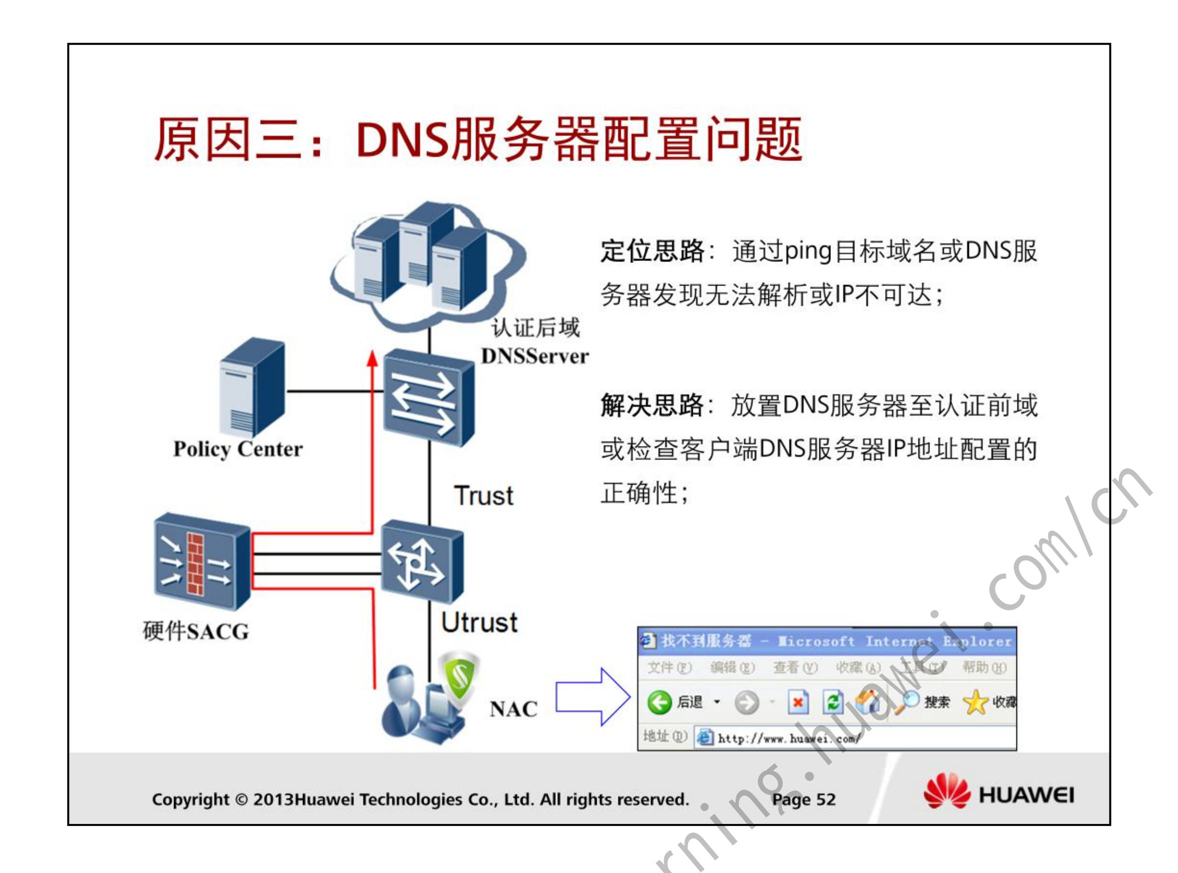
定位思路：通过左图了解，Web推送页面功能只能支持用户浏览器访问Http资源。

解决思路：在IE浏览器输入http协议网站。

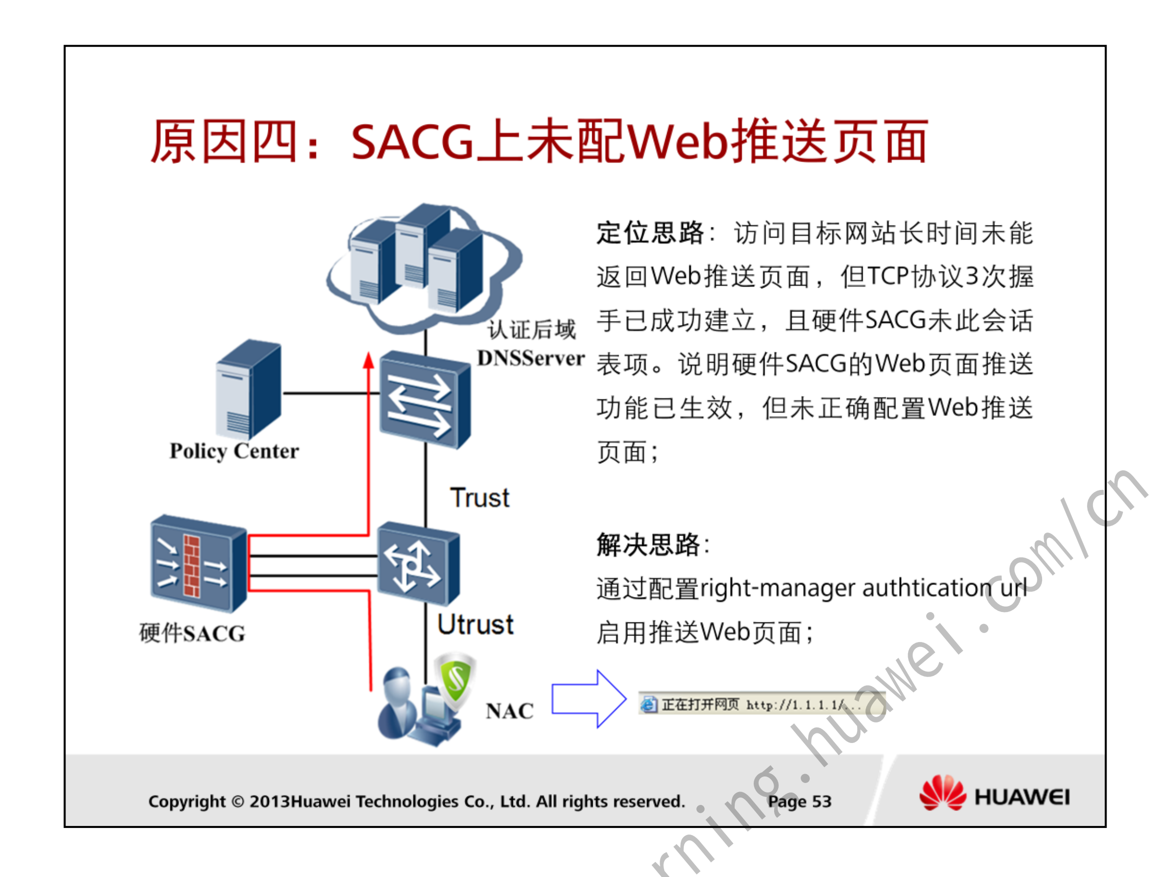
- 通过以上图示可以看出，Web推送页面功能只能支持客户用户使用浏览器访问Http协议资源，配置命令如：right-manager authentication url http://192.168.200.11:8443/webauth



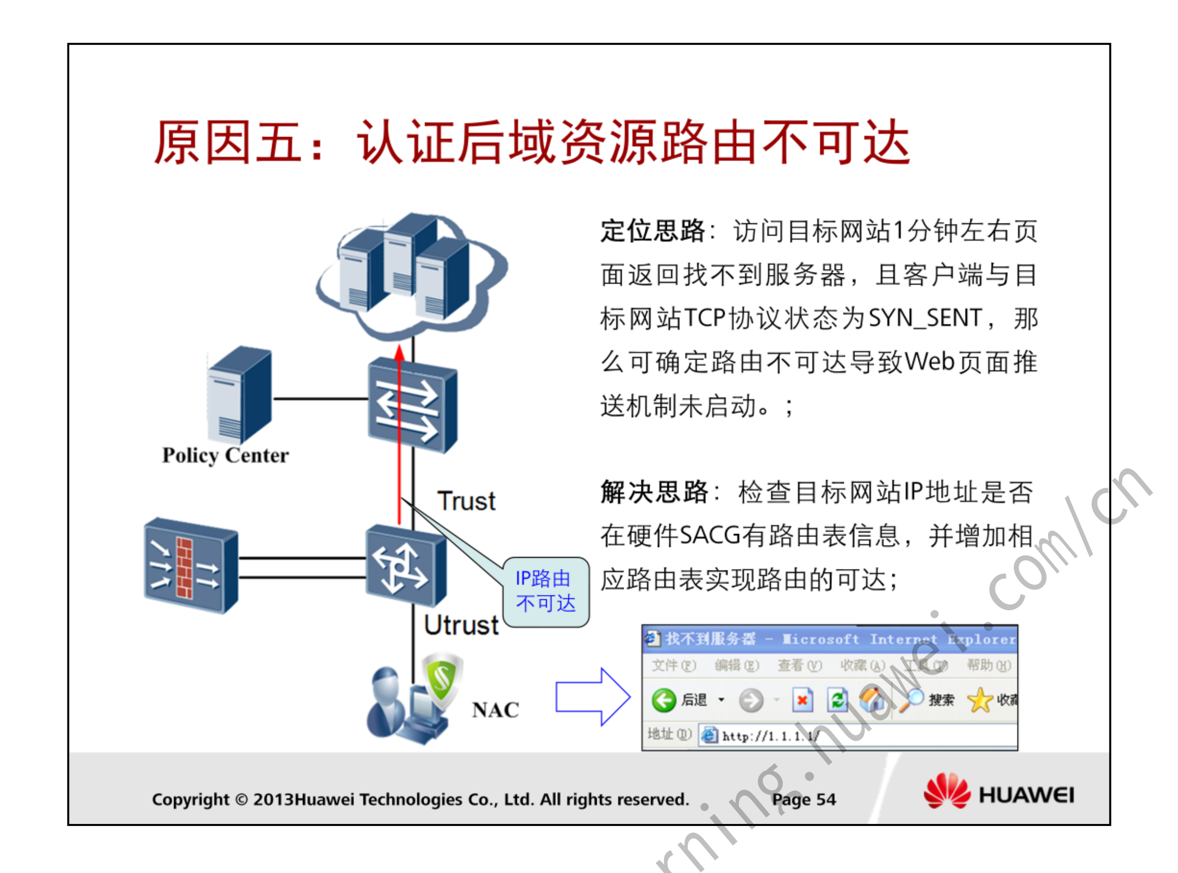
- 非标准HTTP协议端口硬件SACG无法识别为HTTP协议，通过配置端口映射命令port-mapping http port 100 acl 2000，再通过定义ACL2000的源IP地址包过滤策略，就可以实现非标准端口与HTTP协议之间的关联。



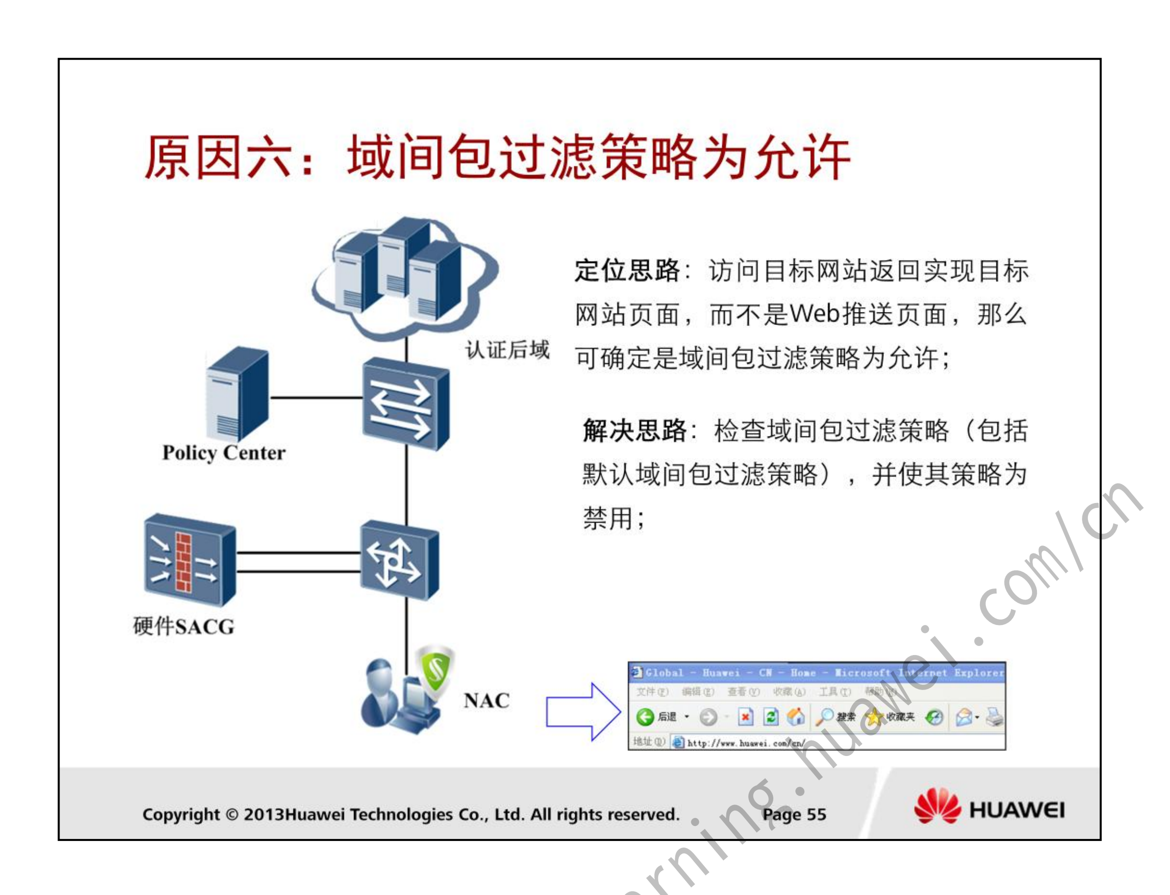
- 通过在IE浏览器输入目标域名，若页面立即提示“找不到服务器”，那么基本可确定是客户端DNS服务器IP地址未配置。若页面经过一段时间后才提示“找不到服务器”，那么基本可确定是DNS服务器IP不可达或客户端DNS服务器IP地址配置错误所致，更有甚者是DNS服务器未含本域名记录或本DNS服务器与上级DNS服务器之间互通性存在问题。
  - 针对页面立即提示“找不到服务器”的情况，需在客户端上配置DNS服务器IP地址，且确保配置正确。
  - 针对页面经过一段时间后才提示“找不到服务器”的情况，需确认DNS服务器是否放置在认证前域和检查客户端的DNS服务器IP地址配置是否正确。



- 访问目标网站若长时间未能返回Web推送页面时，可通过c:\natstat –ano查看TCP协议建立状态。若发现客户端与目标网站TCP状态为ESTABLISHED，且通过在硬件SACG是执行display firewall session table发现客户端与目标网站无任何相应的会话表项，说明硬件SACG的Web页面推送功能已生效，但未正确配置Web推送页面。
- 进入right-manager server-group视图，通过displaythis发现未配置right-manager authtication url启用推送Web页面，通过配置right-manager authtication url http://192.168.200.11/webauth将可以正常启用Web推送功能。



- 访问目标网站1分钟左右页面返回找不到服务器，可通过c:\natstat – ano查看TCP协议建立状态，若客户端与目标网站TCP协议状态为SYN_SENT，那么可确定路由不可达导致Web页面推送机制未正常启动。
- 用户通过http方式访问web资源，SACG需要查找路由来在相应的域间触发web推送。通过在硬件SACG上执行display ip routing查看目标网站的IP地址是否可与当前的路由表信息表项匹配，会发现未找到任何匹配项后通过增加相应路由表项后将可正常启用Web推送功能。



- 访问目标网站返回实现目标网站页面，而不是Web推送页面。通过在硬件SACG上执行display ip routing查看目标网站的IP地址是否可与当前的路由表信息表项匹配，会发现未找到任何匹配项后通过增加相应路由表项后将可正常启用Web推送功能。

本章总结

1. 了解常见的故障排除思路
2. 常握故障排除工作及使用方法
3. 了解文档安全系统组成
4. 文档安全组网方案





思考题

- 终端主机通过身份认证但没有通过安全认证，但可以访问认证后域，分析可能原因有哪些?
- 某出差员工出差在外（不能接入公司内网）要打开某工作文档，但无法打开可能是哪些原因造成?
- 采用硬件SACG接入控制方式组网部署，终端不能访问前域资源，简述故障分析思路及可能原因有哪些?



练习题

- 多选题
  1. 在Policy Center安装过程中提示“连接数据库失败”，导致无法安装。登陆数据库服务器，发现SqlServer正常。可能的原因有?

     A、没有开启远程连接

     B、MSSQLSERVER协议未启用或端口设置有误

     C、数据库密码设置错误

     D、未安装IIS组件
- 单选题

  1.配置以下哪条命令后，在SC和SACG联动失败时将开启逃生通道?

  A、right-managerstatus-detectenable　　B、default acl 3099

  C、right-managerserver-groupenable　　D、server ip 1.1.1.1



- 习题与答案：

  1、在Policy Center在安装过程中提示“连接数据库失败”，导致无法安装。登陆数据库服务器，发现SqlServer正常。可能的原因有?

  A、没有开启远程连接

  B、MSSQLSERVER协议未启用或端口设置有误

  C、数据库密码设置错误

  D、未安装IIS组件

  答案：AB

  2、配置以下哪条命令后，在SC和SACG联动失败时将开启逃生通道?

  A、right-managerstatus-detectenable

  B、defaultacl3099

  C、right-managerserver-groupenable

  D、serverip1.1.1.1

  答案：A

Thank you

www.huawei.com

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：*关联证书*后，请提交您的“华为账号”和注册账号的“email”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见*LVC排期*
- **4、学习工具 eNSP**
  - eNSP (Enterprise Network Simulation Platform)，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）

